Consumers e-Health Alliance Submission to the Joint Select Committee Inquiring Into CyberSafety For Senior Australians

Background

The Consumers e-Health Alliance (CeHA) is an alliance comprising 22 leading chronic illnesses and conditions organisations (Attachment 1).

CeHA notes that several submissions and presentations to the Inquiry into cyber safety for senior Australians have given attention to the impending launch of the Personally Controlled Electronic Health Record (PCEHR).

It is apparent that the terms of reference of this inquiry are particularly relevant to the development of the electronic health record and we appreciate the opportunity to comment on this important issue.

Summary of recent activities relating to the PCEHR

The National eHealth Transition Authority (NEHTA) conducted a stakeholder summit on 12/13 April 2012 and prior to this held a pre-summit consumer workshop on 3/4 April. CeHA representatives participated in both these events.

The proposed PCEHR governance arrangements and the combined issues of safety, security and privacy along with the actual content of one's record were the principal aspects to attract the attention of attendees. Consumers, including senior Australians will want to choose whether to "Opt-In" to such a record.

Former Australian Privacy Commissioner, Mr Malcolm Crompton, made the point in support of the "Opt-In" decision, that an "Opt-Out" approach could not be justified whilst ever the current top down governance arrangement was preserved. This is a view which CeHA strongly supported in its submissions to the Senate Inquiry into the proposed PCEHR legislation.

Issues of concern

The consumer community was not adequately consulted prior to the release of the proposed underlying rules and regulations for the PCEHR and these are now held in dispute by many stakeholders because they are very heavy-handed for a system which has not yet even completed its design phase. They do not keep things simple, an objective which has been CeHA's catchcry, but rather make a currently widely accepted process unduly complex for all parties.

CeHA is very concerned about the risk of cyber fraud upon the aged community who are to be a priority group for PCEHR take up. Our concern has also been very widely expressed by other organisations through their submissions to this inquiry, but we particularly draw attention to those by Australian Federal Police (No. 20), Australian Institute of Criminality (No. 12) and Australian

Crime Commission (No.9).

Furthermore, it seems to us that the DOHA, NeHTA and Telstra inputs to the cyber safety inquiry reflect a self-protective bias which fails to recognise their responsibility to educate the emotionally susceptible senior citizen community (amongst others) on how to use the system safely to guard against the very great risks involved in exposing their health records to unauthorised scrutiny. For example, it is now common to receive a stream of scam emails seeking information from consumers about log-in details to entities such as banks, telcos and the like. Just imagine the potential harm for vulnerable aged people that could arise from their unwitting release of information that would provide such accessibility to their Health Record, let alone access to their normal financial interactions in daily life.

In addition, there is community concern about the possibility of hacking into health record repositories or unauthorised access for improper purposes, but there should possibly be even more concern about "identity fraud." We refer to this only as an example of many issues, known and probably unknown, which have not yet surfaced in part due to the lack of quality cross community consultation but concern about which exists across the community. Our pleas about this are not new but apparently are not heard or understood within government. This has long been a global problem which has not been recognised within the implementation of this critical e Health tool. It is an issue which has been assigned resolution within the dominant technology silo when it is one that deserves broader public policy attention and understanding.

It is also timely to ask what national clinical safety governance for e-health should look like in Australia, as e-health can sometimes lead to patient harm or death through problems in design or operation. This concern is very aptly illustrated by an editorial "A Call for National e-Health Clinical Safety Governance"[1] in the Medical Journal of Australia editorial of 16 April, 2012 written by eminent academics and clinicians: Enrico Coiera, Michael Kidd and Mukesh Haikerwal (Attachment 2).

The authors note that when harm occurs, it may extend to large groups of patients as the result of a single error. They also note that e-health is currently unregulated and unmonitored in Australia and there is no organisation with either the expertise or mandate to govern system safety. They argue that only by governments committing to a set of principles to safeguard whole of system safety can an eHealth system be adequately managed.

CeHA is also concerned about the broader scope of the proposed initial governance of the PCEHR which places all aspects of system operation in the hands of the Secretary of the Department of Health and Ageing (DOHA). Whilst there is some mention of a review to enable community involvement in governance after two years there is little comfort in having the system operator report to an internal and merely advisory governance process until an independent governance entity can be conceived and implemented. To have all performance aspects including content quality, safety, security and privacy operating within the same overall governance structure cannot be regarded as good practice.

Conclusion

CeHA recommends that the Joint Select Committee notes the breadth and depth of issues surrounding cyber safety for senior Australians in eHealth, and encourages the government to hasten slowly in its implementation of these new technologies. We also hope that better

1 https://www.mja.com.au/journal/2012/196/7/call-national-e-health-clinical-safety-governances

governance arrangements can be put in place to ensure that all risks relating to safety and security of seniors' information in the emerging e-health environment can be fully recognised and satisfactorily addressed with due collaboration with the community.

In this context we are recommending that "**the PCEHR Legislation and Regulations be amended so that the proposed Independent Advisory Council advises the Minister, rather than advising the System Operator.**"

--OOO ---

Attachment 1

Introduction to Consumers e-Health Alliance

The Consumers e-Health Alliance (**CeHA**) is not formally incorporated at this stage, but its current partners comprise 22 leading chronic illnesses and conditions organisations along with some individual members. Refer below for listing of CeHA Associates.

Peter Brown – Cancer Voices Australia - convenor.

Steering Committee

Peter Brown (Cancer Voices Australia)

Russell McGowan (Health Care Consumers Association)

Anna Williamson (Leukaemia Foundation of Australia)

Eric Browne, carer (formerly involved with Health*Connect*)

Dr Janet Wale (Cochrane Consumer Network)

CeHA is a collective of consumer oriented organisations and people who have displayed active positive interest in the e- Health program. Our initial activities are to highlight the major blockages to effective implementation i.e. Ownership, Governance, Leadership and the community wide 4C's:-

Communication | Co-operation | Collaboration | Coordination.

CeHA seeks agreed standards at all levels and for all affected community sectors to be appropriately represented at the same table at the same time. CeHA provides the avenue for the tabling of ideas, concerns, needs, information on e-health in which development we have a common interest and which directly affects the individual lifestyles of every citizen including their individual health needs at all times.

CeHA ASSOCIATES as at 1/4/2012

Alzheimer's Australia	Health Consumers Queensland
Aged Care Association Australia - NSW	Health Consumer Council - WA
Arthritis Australia	Health Consumers of Rural and Remote Australia
Asthma Foundation	Kidney Health Australia
Australian Diabetes Council	Leukaemia Foundation of Australia
Australian Lung Foundation	National Heart Foundation
Cancer Council Australia	National Stroke Foundation
Cancer Voices Australia	PRA Mental Health Recovery
Cochrane Consumer Network	Private Mental Health Consumer Carer Network (Australia)
Health Consumers Alliance - SA	Tasmanians with Disabilities
Health Care Consumers Association - ACT	The Country Women's Association of Australia

Editorials

A call for national e-health clinical safety governance

The benefits of technology should not be overshadowed by avoidable patient harm

Enrico W Coiera
MB BS, PhD,
Director, Centre for Health Informatics, Australian Institute of Health Innovation[1]

Michael R Kidd
AM, MB BS, PhD,
Executive Dean, Faculty of Health Sciences[2]

Mukesh C Haikerwal
AO, MB ChB, FRACGP, DipIMCRCS,
Professor, School of Medicine[2]

1 University of New South Wales, Sydney, NSW.
2 Flinders University, Adelaide, SA.

e.coiera@unsw.edu.au

doi: 10.5694/mja12.10475

Well designed and implemented information technology (IT) can lead to safer and more effective clinical care.[1] This rationale has triggered a rapid and unprecedented expansion in e-health investment globally, most recently in national-scale systems. However, e-health can sometimes lead to patient harm or death through problems in design or operation.[2] Chances of harm increase with known risk factors such as poorly designed software or its implementation, including rapid deployment, and poor training and support.[3] We have previously argued for regulation of clinical software to mitigate these hazards; a case echoed internationally.[4-6]

The United States Institute of Medicine recently issued a major report on e-health safety.[7] It recommends the US Food and Drug Administration immediately develop a framework for regulating IT, including standards for e-health manufacture, and the establishment of a new federal entity to monitor, investigate and report patient harms. The US government has agreed to act rapidly on these recommendations.

It is time to ask what national clinical safety governance for e-health should look like in Australia. E-health is now pervasive. Almost every general practice and community pharmacy is computerised. Most public hospitals are in various stages of computerisation, and our first national-scale electronic record system, the personally controlled electronic health record (PCEHR), is due from 1 July 2012. The handful of studies of e-health safety in Australia all point to clear evidence of past harms and future risks.[8-12] Yet there are few working international clinical safety governance examples to follow.

At present, e-health in Australia is unregulated and unmonitored. There is no organisation with either the expertise or mandate to govern system safety "from bits to bedside". Our National E-health Transition Authority (NEHTA) develops health IT standards and specifications and assures their safety. Its Compliance, Conformance and Accreditation program defines the tests that should be applied to certify clinical systems using these standards and specifications. However, it is beyond NEHTA's remit to actually test the safety or compliance of clinical systems or their operation. The Australian Commission on Safety and Quality in Health Care has an interest in the safety of clinical decision-support software but has no regulatory mandate. The Therapeutic Goods Administration, which does have regulatory power, considers clinical software beyond its scope. It may be that e-health clinical safety governance needs to fall under the remit of Australia's Chief Medical Officer, or a specifically designated body.

As they are a new class of IT with an unknown hazard profile, national-scale systems like the PCEHR pose a particular challenge. We cannot quantify today what will result in terms of either benefit or risk. Our capacity to predict outcomes is also hindered because these systems will be used by both clinicians and consumers. What can be said is that there is some evidence that well targeted e-health systems can deliver significant benefits.[1] We also know there is a finite risk of patient harm associated with the use of clinical IT, and that this grows with increased system complexity and usage.[3]

Given the systemic nature of national e-health, harm events will not be confined to individuals and may affect large groups of patients. What would a patient safety incident look like after the launch of the PCEHR? What would happen, for example, if drug allergies were incorrectly uploaded from local clinical systems, or if medication names and doses were somehow incorrectly imported and displayed? Most such informational errors lead to no harm or are picked up by system "defences", such as clinician vigilance. At some point, however, patient harm will occur. How many cases need to occur before the problem is detected? Models from infectious disease surveillance suggest that harm events would first need to be recognised as a cluster, signifying an outbreak of public health importance. The duration of the window between the outbreak and its detection determines how many harm events occur before remedial action is undertaken.

The events most likely to harm patients will occur after IT systems are implemented, often from unpredictable chains of low-risk events involving people, technology and fickle circumstance. They may well result from safe components working in unsafe configurations. Certification that individual components meet standards thus does not guarantee that the overall system is safe. These are the clinical safety challenges for all national-scale systems.

As it is not possible to detect all potential risks during system development and implementation, we need risk management strategies for unforeseen risks. Oversight is needed to manage the tasks of monitoring, detection, investigation and remedial action.[13,14] Monitoring may depend on a combination of adverse event notification and proactive automated and human surveillance. As with the airline industry, when harms eventuate, public confidence in the continued use of a system relies heavily on open

disclosure, as well as rapid investigation and mitigation of the harms so they will not be repeated. We suggest some basic underlying principles for any national e-health clinical safety governance system (Box).

There is currently a gap, stretching from local to national, in safety governance for clinical information systems. While we know something about the risks associated with clinical desktop systems, it is not yet possible to make any definitive statement about whether the PCEHR is safe or not. There is no guarantee that harm events will be rapidly identified or remediated when it is in operation. It is not even clear what safety means for such a system. Even if short-term performance of the new national system turns out to be safe and effective, the international experience suggests that risks will emerge with time. Preventive action to avoid an e-health "air crash" now is a far better option than picking up the pieces after the event.

Acknowledgements: The following have provided constructive feedback and support this editorial: Farah Magrabi, Johanna Westbrook, Ric Day, Siaw-Teng Liaw, Peter Hibbert and Jeffrey Braithwaite at the University of New South Wales; Christopher Pearce at the Inner East Melbourne Medicare Local; William Runciman at the University of South Australia; and Jenny Bartlett at the National E-health Transition Authority. This work is supported in part by funding from National Health and Medical Research Council (NHMRC) Program Grant 568612 and the NHMRC Centre of Research Excellence in E-health.

Competing interests: No relevant disclosures.

Provenance: Not commissioned; externally peer reviewed.

1 Bates DW, Gawande AA. Improving safety with information technology. *N Engl J Med* 2003; 348: 2526-2534.
2 Magrabi F, Ong MS, Runciman W, Coiera E. Using FDA reports to inform a classification for health information technology safety problems. *J Am Med Inform Assoc* 2012; 19: 45-53.
3 Coiera E, Aarts J, Kulikowski C. The dangerous decade. *J Am Med Inform Assoc* 2012; 19: 2-5.
4 Coiera EW, Westbrook JI. Should clinical software be regulated [editorial]? *Med J Aust* 2006; 184: 600-601.
5 Magrabi F, Coiera EW. Quality of prescribing decision support in primary care: still a work in progress [editorial]. *Med J Aust* 2009; 190: 227-228.
6 Sittig DF, Classen DC. Safe electronic health record use requires a comprehensive monitoring and evaluation framework. *JAMA* 2010; 303: 450-451.

Principles for national e-health clinical safety governance

- E-health clinical safety governance must be national but independent of government or industry, to avoid conflicting interests that may lead to resisting change for commercial, professional or political reasons. It must be expert-based rather than organisationally representative.
- Safety is an emergent property of a whole system. Certification of individual components does not guarantee that the whole system is safe.
- E-health clinical safety governance should integrate with mainstream patient-safety processes. Harms arise from sequences of events involving both technical and non-technical elements.
- Governance must assure all components are safe, both alone and in combination with pre-existing elements. Standards and regulatory processes such as accreditation should underpin this, with full legislative backing.
- The safety of the whole system must be monitored in routine use to detect potential risks and actual harm events, as well as clusters. Open disclosure should be paramount.
- Governance must build defences against harm, including safety processes, system redundancies and training, to minimise unsafe use or the creation of unsafe settings.
- Any governance body must have a capability to investigate, analyse and act upon significant risks in the system. ◆

7 Committee on Patient Safety and Health Information Technology; Institute of Medicine. Health IT and patient safety: building safer systems for better care. Washington, DC: The National Academies Press, 2012.
8 Makeham MAB, Saltman DC, Kidd MR. Lessons from the TAPS study — recall and reminder systems. *Aust Fam Physician* 2008; 37: 923-924.
9 Magrabi F, Ong MS, Runciman W, Coiera E. An analysis of computer-related patient safety incidents to inform the development of a classification. *J Am Med Inform Assoc* 2010; 17: 663-670.
10 Sweidan M, Reeve JF, Brien JE, et al. Quality of drug interaction alerts in prescribing and dispensing software. *Med J Aust* 2009; 190: 251-254.
11 Westbrook JI, Reckmann M, Li L, et al. Effects of two commercial electronic prescribing systems on prescribing error rates in hospital in-patients: a before and after study. *PLoS Med* 2012; 9: e1001164.
12 Magrabi F, Li SYW, Day RO, Coiera E. Errors and electronic prescribing: a controlled laboratory study to examine task complexity and interruption effects. *J Am Med Inform Assoc* 2010; 17: 575-583.
13 Singh H, Classen DC, Sittig DF. Creating an oversight infrastructure for electronic health record-related patient safety hazards. *J Patient Saf* 2011; 7: 169-174.
14 Jones SS, Koppel R, Ridgely MS, et al. Guide to reducing unintended consequences of electronic health records. Rockville, Md: Agency for Healthcare Research and Quality, 2011. ❑