PCEHR

By Janine McIlwraith

Does the primacy of privacy come at a cost?

The federal government has invested $467 million in the first release of the personally controlled electronic health record (PCEHR) system.[1] Few could dispute that a nationwide electronic health record (EHR) system has the potential for great benefits in patient care, efficiency and cost.

However, the promised benefits of the proposed PCEHR system may be undermined if the balance between privacy (incorporating personal control) and utility is lost in favour of privacy at all costs. Privacy concerns need to be considered in terms of their potential impact on patient safety. The level of personal control that is appropriate or justified should be determined by a balanced assessment of whether the risks and costs associated with such control effectively outweigh the ability of the system to deliver its intended benefits.

The focus of this article is the tension between privacy – particularly over-arching personal control and unfettered confidentiality – and safety. It does not deal with issues of cost, efficiency and liability. It is also outside the scope of this article to do more than touch on the technical and design aspects of the PCEHR, which perhaps have the largest impact on privacy.

INTRODUCTION

From 1 July 2012, Australians will be able to choose to register for a PCEHR. The Department of Health and Ageing (DoHA) states that the PCEHR is a 'secure, electronic record of your important health information'.[2] The PCEHR is heavily publicised by DoHA as being about improving healthcare by giving 'healthcare-providers the right information at the right time'.[3]

On 12 September 2011, the *Concept of Operations: Relating to the Introduction of a Personally Controlled Electronic Health Record System* ('Conops') was released by DoHA. The document provides an overview of the structure of the PCEHR, the security and privacy principles, the expected benefits of the system and the implementation and adoption of the system.[4] The Exposure Draft of the PCEHR Bill 2011 has also now been released.[5]

Ensuring adequate privacy protection is critical to the PCEHR system. In this regard, the Office of the Australian Information Commissioner has stated that:

> '[g]aining community confidence and trust in the PCEHR System (the System) is essential to its success. While individuals may welcome the potential benefits of shared electronic health records, they may be hesitant to participate if key privacy protections are lacking or are not apparent … the assurance that privacy is protected will be fundamental to the overall success of any electronic health record system.'[6]

Obviously, 'personal control' is also central to a PCEHR. The proposed PCEHR system allows every individual to choose whether or not to have a PCEHR. Individuals who choose to have a PCEHR have control over:

- activating and de-activating their PCEHR;
- who accesses the PCEHR (including setting general and limited access to certain information); and
- which information is added and which information is withheld from their PCEHR.[7]

BACKGROUND

Health Information Technology (HIT), such as EHRs, has long been identified as one possible mechanism by which to reduce the numbers of adverse events occurring in healthcare. While e-health is seen as an instrument for improving safety and quality, poorly designed, implemented or used systems can lead to patient harm.[8] For example, the US Food and Drug Administration (FDA) reported six deaths and 44 injuries from 260 software-related incidents in only the last two years;[9] and, in 2008, the US Joint Commission on Accreditation of Healthcare Organizations (JCAHO) published a Sentinel Events alert on Health IT.[10] A recent Australian study demonstrated that 0.2 per cent of all patient safety incidents reported through a voluntary incident-reporting database in one Australian state were computer-related. Thirty-eight per cent of the incidents were reported to have a noticeable consequence but no harm, while 34 per cent had no noticeable consequence.[11]

The issue of the safety of HIT is recognised worldwide and is being proactively addressed in other nations. For example, in the United Kingdom the National Health Service (NHS) Information Standards Board for Health and Social Care has developed and published two standards to apply to software utilised in healthcare settings, excluding that software captured by medical device legislation.[12] In the United States, the FDA is considering regulation of consumer e-health systems.[13]

The safety of e-health is poorly understood, even among researchers, and continues to be a neglected policy area.[14] There is a pressing need to ensure the safety of HIT, especially such large-scale projects as PCEHRs. The risk of serious harm to a large number of Australians arising from clinical software is a significant and as yet unaddressed threat to the National E-Health Strategy.[15]

PCEHR AND PATIENT SAFETY

The DoHA's 'yourhealth' website[16] states that the PCEHR system is about improving healthcare and ensuring safer healthcare. The Conops recognises, among other factors, that 'limited access to health information at the point of care results in a greater risk to patient safety'.[17] However, a number of aspects of the PCEHR system as it is proposed, in attempting to maximise privacy, give rise to patient safety concerns. For illustrative purposes, one such aspect – the impact of incomplete information and inaccurate information – is considered here. >>

The promised benefits of the proposed PCEHR system may be undermined if the balance between privacy (incorporating personal control) and utility favours privacy at all costs.

Incomplete information

The proposed PCEHR system emphasises the ability of individuals to choose what information is and is not added to their PCEHR, and who has access to what information. This level of personal control increases the potential for the records which are presented to healthcare providers to be incomplete and for that incompleteness to have serious consequences for the patient. In addition, such exhaustive control has the potential to devalue the record to such an extent that it will not be a reliable source of information.

Example: Ms A attends her GP who diagnoses depression and prescribes anti-depressants. Ms A requests that this consultation not be recorded on her PCEHR. Ms A later consults a different GP whom she allows access to her PCEHR. The GP asks her what medications she is taking and forgetting that she had requested the anti-depressants not be listed, she tells the GP that they should all be listed on her PCEHR. The second GP prescribes a drug that is contra-indicated in persons taking anti-depressants and an adverse drug reaction occurs.

It is so obvious – that it almost goes without saying – that an incomplete medical record that does not identify major diagnoses and/or all prescriptions has the potential to lead to harm through the prescription of contra-indicated medications. In the above example, a patient concerned about the stigma (perceived or real) attached to mental health issues has unwittingly compromised her own healthcare by denying the GP, whom she has chosen to trust to deliver to her healthcare with reasonable skill and care, the information he or she requires in order to perform that task.

Perhaps this situation differs little from the situation where no PCEHR exists and a patient chooses not to tell a doctor about a medication they are taking. However, to dismiss the safety concerns on those grounds alone fails to take account of the fact that the PCEHR system is meant to increase patient safety, not maintain the status quo or increase the risk.

What about a situation where a patient consents at the time of consultation to have the information added to the PCEHR but later accesses their PCEHR and limits access to that document, or has the document effectively removed from their PCEHR? To access such advanced controls, individuals will first have to undertake an online tutorial aimed at increasing their health literacy and will have to assert that they have reviewed the educational materials before they can access advanced access controls.[18] However, the effectiveness of such generalised information must be questioned. The educational material will not be able to provide situation-specific information to an individual in the way that a healthcare-provider could. In addition, if asserting that they have read the material simply involves patients in ticking a box on a website, it is hard to imagine how this will adequately reflect the potential gravity of their decision.

In such a situation – where a patient is making decisions that may affect healthcare provided to them at a later stage – would it not be better if such decisions can be made only in consultation with the medical practitioner at the heart of the relevant care? Surely involving the healthcare practitioner who advises that a document is appropriate for inclusion in a PCEHR in the decision to remove or limit access to that decision would strike a better balance between privacy and safety?

Nor will the PCEHR alert the healthcare-provider accessing a PCEHR that documents have been removed at the behest of the individual, or that there are documents forming part of the PCEHR to which only limited access is available.[19] The rationale behind this approach is said to be to prevent individuals being pressured into revealing the limited access information.[20] A simple alert that a patient has seen a doctor and chosen to limit the access to the information concerning that health issue may prompt the healthcare-provider who is seeing that patient to ask the simple question, 'is there any possibility that that document contains information relevant to this consultation?' A conversation could then be had, if necessary, about whether the patient wishes to grant access to that document in the present circumstances. Healthcare practitioners are trained professionals subject to ethical duties; that ethical duty alone should be sufficient to ensure that patients are not unduly pressured into granting access to potentially relevant information.

The Conops document acknowledges that limiting access to clinical documents is challenging and that healthcare-providers have raised concerns over the utility and potential impact of features allowing the individual to limit access to information on their PCEHR.[21] The DoHA has determined that not providing such features may deter some individuals from having a PCEHR, and therefore that such functionality is essential.[22] However, it would seem that there is a relatively compelling argument that not having a PCEHR in such situations may be of less risk to such individuals than having a incomplete, inaccurate record, over which they may have made ill-informed decisions.

Incorrect information

One of the key components of the PCEHR system is the 'shared health summary'. A shared health summary will contain information about an individual's allergies and adverse drug reactions; medicines; medical history and immunisations. The document is created by the individual's 'nominated provider' and cannot be altered by any other

healthcare professional accessing the PCEHR. The nominated provider (in most cases envisaged to be the individual's regular GP) must assert that they are 'delivering continuing, co-ordinated and comprehensive care to the individual' and 'have assessed and described all aspects of the Shared Health Summary and taken reasonable steps to verify the accuracy of information'.[23]

Example: Mr B consults his cardiologist who prescribes a new medication for Mr B. The cardiologist creates an event summary which is uploaded to Mr B's PCEHR, with Mr B's consent. Mr B's GP is his nominated provider. Mr B has no need to consult his GP for nine months after his consultation with the cardiologist. Mr B does, however, see his urologist and oncologist during the intervening nine months. During the period in which Mr B sees his urologist and oncologist, his shared health summary does not reflect the cardiologist's diagnosis of coronary artery disease or the new medication prescribed.

The Conops recognises that allowing only the nominated provider to alter the shared health summary has potential disadvantages in terms of accuracy, completeness and currency. However, the DoHA has decided to adhere to that model and address the possible shortcomings by offering a consolidated view option, whereby the shared health summary is presented alongside information from other clinical documents created since the shared summary.[24]

This approach seems to give inadequate weight to the importance of the accuracy and currency of the information contained in the PCEHR. The Conops does not comment on what the perceived disadvantages are of allowing each qualified healthcare-provider with access to an individual's PCEHR to update the shared health summary, particularly major diagnoses and medications. It would seem that allowing the healthcare-provider responsible for each aspect of an individual's care the right to access and alter the shared health summary would provide a more accurate and timely document. Conversely, it is difficult to imagine how this would detract from the individual's privacy.

OPT IN v OPT OUT

The PCEHR is to be an opt-in system, reportedly to reflect the importance of individual choice and privacy.[25] During the consultation phase, many stakeholder groups expressed their concern that such a system would decrease consumer uptake and consequently decrease the utility and efficiency of the PCEHR system as a whole, thus creating a disincentive for healthcare-providers to participate.

In addition, the Legislative Issues panel has stated that the PCEHR is not intended to be a clinical document, and therefore healthcare-providers should not rely on the PCEHR, but will be responsible for obtaining and maintaining their own records for each patient.[26] Consistent with that approach, the Conops states that the PCEHR is >>

not a replacement for normal communication between an individual and their healthcare-provider.[27] This approach fails to define with sufficient detail just what a practitioner's responsibility will be.

Some authors suggest that decreased efficiency caused by inadequate EHR systems may have the potential to adversely affect patient safety.[28] It would seem logical that the more widely adopted, utilised and comprehensive the PCEHR system is, the more utility it will have and the greater advantage and benefit it will produce. An opt-out system is not contrary to the idea of personal control or the primacy of privacy. If a PCEHR system was automatically created for every Medicare cardholder on 1 July 2012, then an individual's privacy and control could be maintained by allowing that individual either to opt to have the PCEHR deactivated, or simply by not authorising the upload of any information to the record.

DESIGN

In addition to the policy position discussed above, safe design, implementation and use of the PCEHR is required to address potential risks arising from incorrect, incomplete and missing information.[29] The Conops and Legislative Issues Paper do not state with any specificity what design measures have been included to prevent the possibility of information being accidentally transcribed or uploaded to the wrong person's records (as has been seen to occur with other types of HIT). Neither do they comment on what training is proposed to ensure that any risk of such events is minimised. In the UK, efforts are made to ensure the safe design of systems utilised by the NHS via the required compliance with two safety standards that take a safety case approach. In the US, government financial incentives are available to providers only where they purchase EHR systems that meet specified certification standards.

If the federal government in Australia is the entity commissioning the design and implementation of the PCEHR, what mechanism will aggrieved consumers have for seeking compensation if it fails to take reasonable steps to ensure the safety of the system? Holding the manufacturer of the PCEHR system accountable for poor design or other software flaws that result in patient harm might pose difficulties if the federal government has not been specific enough in its requirements for design and implementation standards.

CONCLUSION

In conclusion, ensuring the safety of individuals choosing to opt in to the PCEHR system should be every bit as high a priority as ensuring their privacy. However, it would seem that while privacy issues have been given significant consideration in the Conops and Legislative Issues Paper, safety issues have not received similar consideration. The potential for harm if safety issues are not addressed is well-documented, and other nations are currently working towards ensuring that appropriate measures are in place to ensure adequate government oversight. In implementing the PCEHRs, patient safety must be paramount.

Notes: **1** Australian government, Concept of Operations: *Relating to the Introduction of a Personally Controlled Electronic Health Record System*, 12 September 2011, p11. **2** See http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/pcehr, accessed 23 October 2011. **3** *Ibid.* **4** *Ibid.* **5** See http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/pcehr-legals. **6** Office of the Australian Information Commissioner, *Draft concept of Operations: Relating to the Introduction of a Personally Controlled Electronic Health Record System Submissions to the Department of Health and Ageing*, June 2011, accessed 21 October 2011 at http://www.oaic.gov.au/publications/submissions/2011-06%20Submission%20on%20PCEHR%20ConOps%20FINAL.pdf. **7** Australian government, Concept of Operations: *Relating to the Introduction of a Personally Controlled Electronic Health Record System*, 12 September 2011, p15. **8** F Magrabi, M Ong, W Runciman, E Coiera, 'An analysis of computer-related patient safety incidents to inform the development of a classification'. Submitted for publication in *Journal of the American Medical Information Association (JAMIA)*, July 2009. J Ash, M Berg, E Coiera, 'Some Unintended Consequences of Information Technology in Health Care: The Nature of Patient Care Information System-related Errors', *JAMIA*, (2004)11: 104-12. E Coiera, J Westbrook, 'Should Clinical Software Be Regulated?' *Medical Journal of Australia* (2007) 184(12): 600-1. E Coiera, J Westbrook, J Wyatt, 'The Safety and Quality of Decision Support Systems', *International Medical Informatics Association, Yearbook* (2006). **9** *American Medical News*, 22 March 2010. **10** J Shuren, Testimony to Health Information Technology (HIT) Policy Committee Adoption/Certification Workgroup, 25 February 2010. **11** Magrabi et al, see above note 8. **12** Health Informatics, Application of clinical risk management to the manufacture of health software (formerly ISO/TS 29321:2008(E)) DSCN14/2009 and Health Informatics – Guidance on the management of clinical risk relating to the deployment and use of health software (formerly ISO/TR 29322:2008(E)). DSCN18/2009 More information is available at: http://www.connectingforhealth.nhs.uk/systemsandservices/clinsafety/dscn/index_html/?searchterm=safety. **13** See http://www.fda.gov/ForConsumers/ConsumerUpdates/ucm263332.htm, accessed 21 October 2011. See also: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm263280.htm. **14** F Magrabi, E Coiera, 'Quality of prescribing decision support in primary care: Still a work in progress', *Medical Journal of Australia* (2009) 190(5) 227-8. **15** KW Goodman, ES Berner, MA Dente, B Kaplan, R Koppel, D Rucker, DZ Sands, P Winkelstein, 'Challenges in ethics, safety, best practices, and oversight regarding HIT vendors, their customers, and patients: a report of an AMIA special task force',. *Journal of the American Medical Information Association* (2011);18(1):77-81. **16** http://www.yourhealth.gov.au. **17** Australian Government, Concept of Operations: *Relating to the Introduction of a Personally Controlled Electronic Health Record System*, 12 September 2011, p11. **18** *Ibid*, p72. **19** *Ibid.* **20** *Ibid.* **21** *Ibid.* **22** *Ibid.* **23** *Ibid*, pp50-1. **24** *Ibid.* **25** *Ibid*, p29. **26** Communication with the Panel during the Legislative Issues Paper briefing in Canberra on 26 July 2011. **27** Australian Government, Concept of Operations: *Relating to the Introduction of a Personally Controlled Electronic Health Record System*, 12 September 2011, p22. **28** J Patrick, 'A Critical Essay on the Deployment of an ED Clinical Information System – Systemic Failure or Bad Luck'. Opinion Editorial Draft available at http://www.it.usyd.edu.au/~hitru. **29** JS Ash, M Berg, E Coiera, 'Some unintended consequences of information technology in health care: The nature of patient care information system-related errors', *Journal of the American Medical Information Association*, (2004); 11(2): 104-12. E Coiera, J Westbrook, J Wyatt, 'The safety and quality of decision support systems', *Methods of Information in Medicine*, (2006); 45(1): 20-5.

Janine McIlwraith *is an associate with Catherine Henry Partners and is currently undertaking a PhD at the Australian Institute of Health Innovation at the University of NSW.* **PHONE** *(02) 4929 3995* **EMAIL** *janinem@chpartners.com.au.*