CANADIAN EMR http://www.canadianemr.ca/index.aspx

Frontline News from CanadianEMR for February 24, 2011

A Delicate Balance - Privacy | Access | Data Stewardship

Concerns about data privacy tend to wax and wane depending on the flavour of the moment. Budgetary cuts, funding announcements, missed EHR adoption targets, EMR adoption challenges and the odd eHealth scandal thrown in for good measure all seem to create enough noise to push privacy into the back seat. However, this is usually temporary and privacy 'the elephant in the room' always seems to make its way back into the headlines in some form or another.

Protecting the privacy of personal health information is complex and challenging. If there were simple answers, there would be no debate and more importantly, no need for debate. The truth being that there is more than one right answer to each question.

Last week, I was directed to an article in University Affairs (Cardwell - Exploring the glitches in the system) which described some of the work done by sociology professor Gary Genosko, holder of the Canada Research Chair in Technoculture at Lakehead University. Much of his work has focused on understanding the actions of individuals and small groups to subvert or disrupt mainstream information systems and infrastructures.

Cardwell states*: Dr. Genosko likens those "acts of sabotage" to today's WikiLeaks phenomenon and what he calls "the crumbling of the distinction between classified and declassified information." They also tell us something "about how people react to technological innovation [and] how they transit to becoming part of the system. To me that is interesting and highly relevant today because information technology is ubiquitous and is changing fundamentally the way we live."*

Cardwell also describes a fascinating example of state driven data collection that (although well intended), crossed the boundary of individual rights repeatedly through the collection of information on liquor sales in Ontario over a 50 year period. Dr. Genosko calls this concept "the informatics of subjugation," and in his book Punched Drunk: Alcohol, Surveillance, and the LCBO, 1927-1975, "examines efforts to monitor and control alcohol consumption through an elaborate surveillance bureaucracy that gathered and shared personal data on thousands of individuals."

So, what lessons can we apply with respect to privacy and protection of personal information in the era of EHRs, EMRs, Repositories, Shared records and inter-connected healthcare systems?

We sit at the interface between what used to be 'classified information' protected by cardboard folders in locked record rooms and medical practices and the new world of web-based access to vast quantities of personal information that were not previously accessible.

How do we proceed and learn without making gargantuan errors that put untold numbers of personal records at risk? We do not know all the answers and there must be room for some level of experimentation or we risk getting it badly wrong.

There is another facet that has been conveniently ignored by government in particular. That is the need to have informed and open debate about the issues at stake through consultation with the public, care providers and health system administrators. There has been some discussion with the 'managers' but very little transparent debate with the public.

We have to get the fundamental principles right or we face both risk and the enormous financial and policy risks of mis-stepping.

For example, in January 2011 the Canadian Medical Association released a privacy policy document 'Principles for the Protection of Patients' Personal Health Information'. In the document, the CMA states, "Patients should be informed that the treating physician cannot control access and guarantee confidentiality for an electronic health record (EHR) system". The policy goes on to state that "Implementation of an interoperable EHR requires a strict privacy framework, including an access audit "trail" to safeguard against unauthorized access. Patients should be able to access this audit trail."

If a doctor cannot safely control access and guarantee confidentiality of information in an electronic health record system used to deliver daily care, to quote a phrase, 'something just aint right'.

What are your thoughts about privacy and the protection of personal health information? Add by clicking on the 'Comments' link below

Posted by Dr. Alan Brookstone on February 19, 2011 at 12:25 PM in E. Privacy Issues | Permalink