Ontario health records proposal would breach privacy, experts say

The province of Ontario is contemplating the creation of electronic health records that could include a patient’s psycho-social, financial and legal history, a provincial official has indicated.

But so comprehensive and sweeping is the proposed database that privacy and legal experts say they are “appalled” and “stunned.”

The province’s plans, sketched at an e-Health conference in Toronto, Ontario earlier this month by Grant Gillis, director of ehealth standards for eHealth Ontario, would see the creation of comprehensive profiles about all Ontario patients, including their “social history.”

The records could include information about a patient’s education, employment, financial status, legal history, residence history, sexual orientation and spirituality, Gillis told the conference. Gillis also indicated that the information could include a category called “risk.” eHealth Ontario later indicated in an email that risk is a “general” category. Some examples found on forms provided by stakeholders during our engagement process include: Risk of falls/wandering; Risk of harm to others; (and) Risk of patient having perhaps been exposed to an infectious disease.”

The aim is to create “an overall clinical information model for Ontario,” Gillis said.

In response to an inquiry about the appropriateness of including some manner of legal and psychological risk profile in the health profiles of the province’s 13 million residents, Gillis said the risk category had been included in the template after early consultations with clinicians and other stakeholders. He added that access to the records would be carefully controlled by state-of-the-art computer confidentiality barriers, and that information included in the social history category of the electronic health records would not necessarily be accessible to everyone. Only “authorized persons” would likely have the right to access parts of the health record containing sensitive information about a patient’s risk assessment or legal history, he said.

The latter reassurance is unconvincing, says Khaled el Eman, Canada Research Chair in Electronic Health Information at the University of Ottawa’s Faculty of Medicine in Ontario.

The notion of huge government patient health databases that include psycho-social profiles is highly problematic, he says. “A big concern would be how this data would be used or disclosed for secondary purposes once it is collected. This is not an issue that is being discussed, but once the data is there, it can be used [in] many unanticipated ways and it is not clear what controls there would be on these secondary uses and disclosures, if any. Should one go by precedent, there may not be many constraints or controls.”
The government must clarify who will have access to the electronic health records, el Eman adds. “I think if this information is collected, patients would expect it to be available only to their treating physician. If it is available at tens of thousands of points of care then I think that would erode public trust in EHRs/EMRs pretty quickly. That is, if the public is actually informed about this. But then it will take just a few data breaches or misuses for the story to come out.” (Editor’s note: Canada Health Infoway views the concept of Electronic Health Records or EHRs as being completely distinct from Electronic Medical Records or EMRs. The former refers to the national electronic architecture, says the agency, which argues that the development of an “interoperable” national infrastructure is its primary responsibility. When completed, that national architecture would primarily be used to aggregate health information in such a way that it would be valuable for policymakers and researchers. The latter concept, EMRs, by contrast, is seen as recordkeeping systems at the doctor–patient level that would be used primarily as an aid in the clinical diagnosis and treatment of disease).

Information and Privacy Commissioner of Ontario Ann Cavoukian said in a statement prepared for CMAJ that she has contacted Greg Reed, CEO of eHealth Ontario, to discuss the proposed health records. “He assured me that they will be consulting with my office on possible data fields that practitioners have expressed interest in,” Cavoukian writes. “Nothing will be finalized until my office and other privacy specialists are consulted. One thing is clear – patient privacy must be directly embedded into the design of our electronic health records from the outset, not as an afterthought.”

The rationale for including a patient’s legal history in the records and an ill-defined category for “risk” is confounding, says Michael Power, a lawyer who served as vice president for privacy and security for eHealth Ontario between 2007 and 2009.

Power was “stunned” to learn of the proposed information categories and is unconvinced that access will be limited to those with a need to know. “The system is designed to provide the maximum access to the maximum numbers of persons.”

The data to be included in EHRs is “the thin end of the wedge of a much larger question,” Power adds. “That question is whether these records are appropriate at all.”

Comprehensive electronic health records available province- and nation-wide would have limited, if any, value to clinicians, whose essential needs are basic health information about the patient and his condition, Power argues. “What governments are building doesn’t match the needs of healthcare providers. … It feels like a white elephant.”


Inclusion of “social history” information about patients within electronic health records is “very worrying,” says Trisha Greenhalgh, director of the Healthcare Innovation and Policy Unit at The London School of Medicine and Dentistry.

Information about medication, allergies and adverse reactions represent the ‘hard’ or codifiable end of the data spectrum within EHRs but eHealth Ontario’s social history category clearly “includes material that is ‘soft’, context-dependent and potentially contestable,” she says.

In the UK, there has been a backlash to government efforts to introduce records containing extensive personal profiles, Greenhalgh says.
eHealth Ontario conducted public consultations on its specifications for the new health records last January and published a list of parties who responded. Those included some health institutions and technology companies but not legal, privacy or civil rights experts (www.ehealthontario.on.ca/programs/clinicalDocument.asp).

The Office of the Information Commission of Ontario was not aware of the consultations at the time, spokesman Angus Fisher says.

Nor had el Eman heard of the consultations. “I would be surprised if there was a real public consultation that no legal and civil liberty groups would have responded or reacted,” he says. — Paul Christopher Webster, Toronto, Ont.

Editor’s note: Twenty second in a series on electronic health records