

Electronic Health Records as a Threat to Privacy

Glenn Griener

Introduction

Governments across Canada are investing millions of dollars into the creation of electronic health records systems. While these systems offer great promise of improving the nation's health care system, they also pose considerable risks to individual privacy.

In this brief paper I hope to do two things. First, I hope to foster a clearer understanding of the risks. The risks are often misrepresented or misunderstood because of some prevalent misconceptions about the nature of the proposed electronic systems. For that reason, some explanation of the systems is needed. I use Alberta's Electronic Health Record as an exemplar. Once the nature of the risk is delineated, I sketch some of the steps which I believe are necessary for dealing with them.

Alberta's Electronic Health Record – Wrestling with Misconceptions

Discussion of a provincial or national electronic health record (EHR) often conjures up the image of a massive new database created by the government and containing a lifetime of one's health information. This picture is undoubtedly fostered by the loose descriptions which are so often offered by proponents of such systems. But it is mistaken on at least two significant counts.

In the first place, there is no new warehouse of information. Rather, the Alberta's EHR is an electronic network that links the patient records which are collected and maintained by health professionals and by regional health authorities.

The EHR provides a portal through which this information can flow from one care provider to another. Pharmacist Kumar, who operates a community pharmacy, can use his computer to obtain information about a patient from Dr. Lee's record. A crucial point to emphasize is that professional responsibility is maintained by those who have traditionally had responsibility for the collection, use and disclosure of health information. I will return to this point below.

A second common misconception is that *all* information collected by *any* health professional will be made available through the data exchange system. This need not be the case, and at the present time it is not the case. For instance, the information which is currently available through the Alberta Electronic Health Record is merely a subset of the information which is available within Capital Health's netCARE.¹ And the information which is available through netCARE is itself just a subset of information which physicians and clinics in the region maintain within their own records. Simply stated, much of the health information collected in a variety of settings is not available through current electronic health records.

Security and Electronic Health Records

The creation of a network linking databases full of health information, information which most people find to be among the most sensitive, creates some new risks. Hackers may invade the system and view individuals' health information or – far worse – change it. Health records may be lost through computer failures. But electronic databases loaded



with important personal information are now ubiquitous, and dangers such as these threaten all of them. We have developed confidence in our ability to deal effectively with these hazards. Why should we doubt our ability to manage threats to electronic health records using the state-of-the-art technology and practices developed for other arenas of the electronic environment?

Electronic Health Records and Professional Responsibility

As noted earlier, the EHR is not a massive new record; rather, it is a portal for the transfer of patient information. Information is collected and recorded by one health care provider and flows through this network to other health care providers. In one sense, the advent of the system changes nothing. Health care providers – be they individual professionals or large regional authorities – maintain responsibility for their patients’ health information. However, in another practical sense the change is enormous. Professionals will have to think about their responsibilities differently and exercise them in unusual ways.

Individual professionals traditionally exercised their professional responsibility to protect information on a case-by-case basis. Dr. Lee would have to decide whether she should disclose the patient’s diagnosis or laboratory results to Pharmacist Kumar. This decision should turn on whether that pharmacist has a need to know, a need which typically arises from a direct, care-providing relationship with the patient.

The creation of the EHR takes the decision about disclosure out of the hands of the individual provider who collected the information and moves it to a system-wide level.

Once the system’s protocols give pharmacists access to lab results, for instance, individual physicians lose an element of control they have traditionally enjoyed. If Dr. Lee’s personal opinion is that pharmacists do not need this information, she has no effective way to keep her patients’ results

from pharmacists. Additionally, the EHR prevents Dr. Lee from discriminating among the specific professionals to whom she discloses information. If Dr. Lee does not want Pharmacist Jones to have some information but has no objection to Pharmacist Kumar’s access, she has no effective means of putting this into practice.² Once the information is made available to the network, the network’s rules determine who has access.³

One major benefit of the EHR is that professionals no longer need to obtain information through an intermediary, or incur the costs of duplicating tests. They now have direct access to

information collected by others. Given the current design of the system, professionals have access to a person’s information regardless of whether they are in an actual care-providing relationship with that individual. But this is not a new situation created by EHRs. A hospital’s paper charts may be accessed by staff members who are not providing care to the patient. And the ethical principle which should guide decisions does not change. The basic “need to know” principle remains in effect – health professionals

should have access only to information which they need in order to provide care. What has changed is that there is no longer another party to judge that need. The professional with unimpeded access must judge himself or herself, asking whether he or she needs the patient’s information.

Richness of Information in Electronic Health Records

The EHR currently contains a relatively meagre set of information. This fact does not, of course, offer any guarantee about the future. Once these systems are in place we should expect that there will be ongoing pressure to expand the amount of information available through them.

While the richness of information contained in the EHR is likely to increase, there is no reason to succumb to a technological imperative. No one should assume that there exists a preordained endpoint – that the EHR will continue to grow unchecked until it contains all of the information which any

“Why should we doubt our ability to manage threats to electronic health records using the state-of-the-art technology and practices developed for other arenas of the electronic environment?”



health care provider collects during the individual's lifetime.

The EHR will be developed in stages. At each step we can ask whether a certain element of information should be brought within the network. We have no need to decide in advance and, in the absence of any experience, it is uncertain what information should be included. Piecemeal construction of the EHR means that we can solve these issues as a series of specific questions. For example, should specialists' interpretative reports on diagnostic images be made available? What about the images themselves? Laboratory results are now available to physicians, should pharmacists also have access to this information? In answering these questions we should keep an eye fixed firmly on the *raison d'être* of the AEHR – improving the care that patients receive.

Secondary Use and the Need to Know

I have asserted that the reason for creating an EHR is to improve the care that people receive. However, it should be recognized from the start that this is not the only potential use. All of the recent government reports on the Canadian health care system have recommended the creation of electronic health records, and all of these reports, written from different points on the political spectrum, cite improved care as a primary reason for making this costly investment. What is striking about the various commissions is the wide spectrum of additional uses they find for the electronic records. A couple of examples demonstrate this:

An integrated electronic health record that tracks individuals' health along with various treatments, medications, and tests would be an invaluable tool for all aspects of the health system. ... [I]t would provide access to essential information about a person's health, help ensure people get timely and accurate diagnosis and treatment, help track overall use of the health system, and allow better assessment of the outcomes of various health services. The most important benefit is the opportunity to use this information to improve both the health of individuals and the quality of our health care system.⁴

Electronic health records provide aggregate data that can be used in health research and in

health surveillance, tracking disease trends and monitoring the health status of Canadians.⁵

These lists of uses are not, in themselves, particularly worrisome. After all, many of the uses have long been a part of everyday practice without creating breaches of privacy. These uses are often clearly permitted by current health information legislation.⁶ In fact, an electronic system may offer greater privacy protection when these activities are being conducted. When data is maintained in an electronic format it may be much easier to remove unneeded individual identifiers from the information used for purposes such as quality assurance and program evaluation. Moreover, all of these uses can be linked at least indirectly to improvement in health care provided to the individuals whose information is used.

The real danger of expanding uses is, I believe, more subtle. We ought to expect that as the EHR becomes a richer source of information human ingenuity will devise a much wider range of possible uses for the data. We will see more secondary uses proposed. A glance to the South clearly illustrates the point.

A recent report published by a reputable organization in the United States advocates the creation of a national electronic health record as a means of improving patient safety, surely a laudable use. The danger of an EHR becomes manifest when the authors speculate on other potential uses.

Although the focus of this report is on patient safety, it is important to note that the proposed national health information infrastructure will yield many other benefits in terms of new opportunities for access to care, care delivery, public health, homeland security, and clinical and health services research.⁷

Managing the Risks

Electronic health records clearly hold great promise for improving the health care Canadians receive. This promise does not come without some significant risks. We must ultimately decide whether the gamble is worth taking. Can the risks be managed?

One requirement is a renewed sense of professional responsibility. Health care professionals must learn to think about health information in an unaccustomed way. Instead of considering whether they should disclose to others the informa-



tion they control, they must learn to ask themselves whether they should peruse the information to which they have unfettered access. Many will need to overcome the ingrained sense that they have a right of access and use. Licensing authorities will need to use their powers to foster this change.

A second requirement is an open and public discussion about the legitimate uses of health information. Many of the proposed secondary uses have a great initial attraction, but others clearly require that much greater deliberation be carried out in the public setting.

Glenn G. Griener is an Associate Professor in the Faculty of Medicine and Dentistry (Public Health Sciences) and the Faculty of Arts (Philosophy) and holds a joint appointment with the John Dossetor Health Ethics Centre, University of Alberta, Edmonton.

1. Information about netCARE can be found at <<http://www.capitalhealth.ca/Health+Services/Information+for+Health+Professionals/netCARE/default.htm>>. Information about Alberta Electronic Health Record can be found at <http://www.albertawellnet.org/default_ehr.asp>.
2. This does have an important consequence for patients whose family members are health care professionals. Ms. Jones may not want her mother, a pharmacist, to know that she has a prescription for contraceptives.

3. The discussion in this paragraph ignores a couple of important points. In some situations professionals may decide to protect patients by deciding not to participate in the EHR or by deciding against recording information in it. I also ignore the capacity to mask information which is recorded in the system. These possibilities are ignored because they all have serious costs which make them impractical for most situations.
4. Alberta, Premier's Advisory Council on Health, *A Framework for Reform: Report of the Premier's Advisory Council on Health* (Edmonton, Premier's Advisory Council, 2001) at 46 (Chair: Rt. Hon. Don Mazankowski), online: Premier's Advisory Council on Health <<http://www.premiersadvisory.com/reform.html>>.
5. Canada, Commission on the Future of Health Care in Canada, *Building on Values: The Future of Health Care in Canada - Final Report* (Saskatoon: Commission on the Future of Health Care in Canada, 2002) at 78 (Chair: Roy J. Romanow, Q.C.), online: Health Canada <<http://www.hc-sc.gc.ca/english/care/romanow/hcc0086.html>>.
6. See, for example, Alberta's *Health Information Act*, R.S.A. 2000, c. H-5, s. 27.
7. Committee on Data Standards for Patient Safety, Board on Health Care Services, Institute of Medicine, *Patient Safety: Achieving a New Standard of Care* (National Academies Press, 2004) at 8, online: <<http://www.nap.edu/books/0309090776/html/>>.

