Medical Records:
The Interoperability Conundrum

Bill Nikolai
LIBR 516 • UBC - SLAIS • April 2008

Medical Records: The Interoperability Conundrum

Bill Nikolai - LIBR 516 - April 2008 (SLAIS, UBC)

I. Introduction

Perhaps no other health information issue is currently undergoing as much discussion as is that of the development and adoption of national health information networks (NHINs), the lifeblood of which is electronic health records (EHRs). The focus of most of the dialogue - and the source of much debate - is the "interoperability" of such records within these massive networks; it has been referred to as "healthcare's hottest topic ..." (Heubusch 2006, 26). Interoperability (i.e., ready access to an individual's medical information by practitioners and others, from disparate areas and organizations, as well as the patient herself) is both aim and bane to proponents and critics of large-scale networks, respectively. It is the intent of this paper to provide some background and elucidate some of the problem areas and priorities with regard to management of personal health information in this rapidly emerging environment.

II. Records evolution

The management of records documenting patient care underwent a significant change shortly over a century ago: in about 1890 most hospital records began to be created using typescript rather than manuscript. With the move to type from handwriting, there was also a shift to the use of printed forms and a standardization of records, over the ensuing decades (Craig 1990, 60-1).

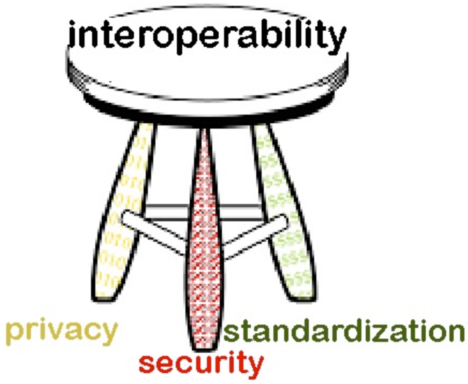
Arguably, the next significant evolutionary step in medical records management (roughly one hundred years after the introduction of typescript) is the effort by individual doctors and clinics to produce computerized "electronic medical records" (EMRs). Because of the plethora of information management systems, many of which are proprietary, it is questionable as to whether this has led to greater standardization, at least in the larger context. In any case, the changeover is ongoing and even today only about 23 percent of Canadian physicians use "some form of electronic medical record" (Buckler 2007). Many doctors are creating both paper and electronic records (for example, if their practices are split between clinics using paper and those that are not); those physicians who are using paper only, however, are either in the process of converting or likely will be imminently, especially given financial incentives from governments and other health care providers to do so (see Greiver 2007 for an interesting account of one physician's experience with the conversion process).

A 2005 editorial in the *Bulletin of the World Health Organization* underscores the urgency with which governments are embarking on initiatives representing the next great phase in the evolution of medical records - the adoption of "electronic health records" (EHRs), which can be distinguished from EMRs by digital standardization enabling widespread access within large, integrated networks. The imperative to move forward with regard to interoperability is framed in the context of social benefits, including significant potential quality of care improvements for patients. However, it is clear that economic benefits to be accrued by hi-tech adopters are seen to be equally - if not more - important:

> ... millions of health care dollars are wasted every day duplicating prescriptions and re-ordering laboratory and diagnostic tests because of lost or misplaced results. In addition to the human costs, these problems ripple through the health care system - affecting waiting times and limited budgets and wasting valuable human resources ... (Alvarez 2007).

III. Creating a context: Surveying the main elements

There appears to be little argument that there are not great advantages to be gained from making medical records accessible electronically to a variety of stakeholders, including patients themselves. At the same time, none would argue that accessibility to personal medical information (with "personal" meaning the identification of individuals with specific records) ought to be unimpeded and open to all. The issues essentially need to be framed in the context of *privacy*, *security* and *standardization* and how these elements can be developed and brought together in supporting interoperable networks that can benefit all stakeholders. Of course, a national health network can only succeed in any measure if the subjects of the records (namely, the patients) "buy in" and have confidence in both the benefits and the security of the system. Failure is almost guaranteed if the network's business practices are not "unambiguous and transparent to the public" (Rhodes 2006, 70), especially in the U.S. context, where patients ostensibly have the choice to opt in or out of various health care schemes. In Canada, where participation in government health care programs is virtually mandatory, the patient is perhaps less a discriminating consumer than a traveler who is along for the ride. (This does not necessarily mean, however, that Canadians are any less concerned about privacy and security issues when it comes to their medical information).



1) Privacy

Patients hope and expect that their medical records are private, meaning that without their consent, physicians and other practitioners cannot pass on or provide access to personal information to any other interested parties.

In the U.S., this privacy principle is enshrined in the 1996 federal *Health Insurance Portability and Accountability Act*, commonly known as the HIPPA law. Among other things, HIPPA's mandate is to protect patients in a number of ways by ensuring that their health insurance and information is portable, private and secure, and that information is handled in a standardized manner.

With regard to privacy, in particular, HIPPA stipulates that one's identifiable medical information cannot be shared without permission in most circumstances, for example, with an employer or for use in advertising or marketing; neither can notes about such things as mental health counseling sessions be shared. Penalties for disclosure of individually identifiable health information in violation of HIPAA are stiff ($50,000 and up to one year in prison).

In fact the Act *does* allow for the use and sharing of patient medical information in a variety of contexts. For example, information can be shared in order to: facilitate coordination of treatment and care and payment for such; inform family, relatives or friends who are caregivers (unless the patient objects); ensure good care on the part of physicians; protect public health; or make required reports to police (such as reporting of wounds suspected as resulting from the use of weapons). (See the United States Department of Health and Human Services, Office for Civil Rights – HIPPA website for more information, including a list of HIPAA-related links and a Privacy Rule summary.)

In Canada, patients' private medical information is protected mainly by the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) (which uses the Canadian Standards Association's *Model Code for the Protection of Personal Information - CAN/CSA Q830/96* - as its basis and is available through the Department of Justice), as well as provincial acts (see a list provided at the Office of the Privacy Commissioner of Canada health links website; this includes legislation such as Alberta's *Health Information Act* [HIA] and B.C.'s *Freedom of Information and Privacy Protection Act* [FOIPPA or FOIPOP]). In addition, the Canadian Medical Association has formulated a privacy code that all physicians in the country have agreed to abide by (see Canadian Medical Association 1998).

2) Security

While privacy legislation and standards address the right of an individual to have anonymity and to vet the transfer of and access to personal information, security refers to the mechanisms supporting privacy. Just because we intend information to be private does not make it so. There must be policies, procedures, tools, technologies and accountability methods in place supporting privacy, as well as the means to enforce laws and regulations by detecting and penalizing contraventions.

3) Standardization

In many ways, the push to enable interoperability in the healthcare world is an enormous task, given the sporadic and piecemeal adoption of information technology by practitioners and organizations in the field to this point. In some ways, the challenges posed by the need to standardize around particular technologies and protocols (which is an obvious key to interoperability) are perhaps fewer in Canada, which has a nationwide system of socialized healthcare, than they are in a country such as the U.S., which has a very fragmented and politically sensitive healthcare scene.

Nevertheless, one need only look to a context such as the U.K., which also has a socialized national health service (NHS), to realize that interoperability is an extremely complex goal from a technological and logistical standpoint. Integration in healthcare there has been characterized as multilevel, with the first level being "one-off, point-to-point integration between local systems," for example, in sharing demographic information among departments within a hospital or other local system. Second generation integration is much more complicated: it might involve meeting demands for "order communications, results reporting, e-prescribing, radiology / PACS integration, e-referral and discharge summary." [PACS refers to picture archiving systems.] Add to that, the fact that many practitioners are beginning to use PDA's at the bedside, as well as the need to be able to interact with other institutions to facilitate electronic referrals, record transfers, social care and telecare, and it becomes clear that creating interoperability is a difficult challenge indeed (A new era in interoperability 2007).

For records managers specifically (as opposed to IT gurus), just a couple of obvious challenges involve the creation of protocols with regard to medical coding (see AHIMA's *Statement on Consistency of Healthcare Diagnostic and Procedural Coding* for a discussion of this important issue: American 2007) and migration of data from one system to another. This may also involve having to develop templates and procedures to map information from one type of record to another, as well as managing any data entry (which will obviously be especially necessary in cases where a shift is being made from paper to electronic records). There is also a need to develop metadata standards for electronic health records. Different practitioners will have differing requirements with regard to what metadata elements they would like to see included in a record; there will also be evolving legal mandates regarding metadata (Geltzer 2008). Lastly - but certainly not least - records managers will have a role to play in designing transparent and understandable output from records for patients, who are being promised access to information about themselves and who are increasingly likely to want to view their own records.

IV. Bones of contention: Problem areas

There are considerable, weighty forces at work hoping to erect interoperability skeletons and put flesh on healthcare records frames. In Canada, government initiatives with regard to eHealth are manifested in the activities of the Canada Health Infoway, a federally-funded organization comprised of the country's Deputy Health Ministers and billing itself as "catalyst for collaborative change to accelerate the use of electronic health information systems and electronic health records (EHRs) across the country" (Canada 2008). In the U.S., the federal Department of Health and Human Services (HHS), through the Commission on Systemic Interoperability, has produced its own corpus - entitled *Ending the Document Game* - which insists that the solution for healthcare inadequacies in America is "to connect healthcare information electronically" (Commission 2005, vii). Non-governmental stakeholders promoting interoperability in the U.S. are represented in the eHealth Initiative and Foundation, whose vision it is to support "ready access to timely, relevant, reliable and secure information and services through an interconnected, electronic health information infrastructure" (Foundation 2008)

Clearly, there are concerted efforts being made to give these integrated systems legs and have them walking imminently. Yet, enthusiastic promotional pitches notwithstanding, serious misgivings about the prudence of rushing too quickly into high-level integration are being expressed by various bodies and members of the public.

Most of the criticism and concern arises out of privacy and security concerns. The authors of *Ending the Document Game* optimistically state:

> While a system of interoperable health information can be designed to carefully monitor the access and use of information, it's not possible to ensure that there are no 'prying eyes.' The limits of safeguards will be determined primarily by the state of technology ... In time, the system will be strengthened with biometrics ... But even the most basic system of connected health information will provide more consistent security and improved tracking of access than any paper system can (60).

Have there already been instances of electronic health record privacy and security breaches? Two cases from the U.K. recently made the news. In one case, the personal medical records of 4,000 NHS patients were lost by an employee who was transporting files on a USB stick clipped to a lanyard that was hanging from the neck of the employee. The loss only came to light publicly after a freedom of information request (Savvas 2008).

While the latter incident involved an accident, another earlier instance of breach of confidentiality was clearly a result of inappropriate actions by medical staff. The records of an unnamed celebrity were viewed by more than 50 staff members who were not participating in the care of the famous patient and thus were not authorized to access the records (Collins 2007).

It’s hard to imagine that had the records in the two examples above been paper, the magnitude of the accident (in the first case) and the extent of malfeasance (in the latter instance) would have been as great. After all, one can’t easily cart around paper copies of 4,000 medical records and then inadvertently drop them; and having more than 50 people trying to spy on a paper record without attracting attention is also not so likely.

Proponents of EHRs and integrated networks would argue that in each case, proper use of existing technology (for example, encrypted file transfer and the vigilant use of audit trails) could have prevented the problems that arose. Yet, they did happen and critics contend that the potential for much larger-scale breaches is there.

Moreover, it would appear that even some insiders are extremely uneasy with more fundamental aspects of interoperability initiatives. The resignation less than a year ago in the U.S. by Paul Feldman, the cochairman of a HHS advisory group on technology, was primarily prompted by serious concerns about a dearth of comprehensive policies on the part of the federal government and HHS with regard to privacy and security issues. Among other things, Feldman, together with other advisers to HHS, pointed to a lack of vigorous enforcement of HIPPA-related infractions as well as an unwillingness to develop policies covering non-HIPPA-covered health records, such as those being collected by some employers, including Walmart (Carroll 2007).

Some of the same concerns were subsequently echoed by Bryon Pickard, President of the American Health Information Management Association (AHIMA) in testimony given to the Subcommittee on Information Policy, Census and National Archives. In addition, Pickard also pointed out that “It is important to define what constitutes health information discrimination” (Pickard 2007, 9). Here the allusion is to the misuse of the personal health information of employees or clients (either present or potential) by employers or insurance companies; Pickard conceded that there may be legitimate needs for information on the part of these organizations, but asserted that more effort must be put into defining what those are (9).

Are citizens really concerned about who sees their medical information and how it is subsequently used? Certainly, in the U.S., where having or not having medical insurance can ultimately be a matter of financial solvency or even of life and death, individuals have much at stake in what happens with their records. Fear of being denied insurance on the basis of health record discrimination is palpable among some people who are avoiding genetic and other medical investigations because of what testing might reveal and thus leave in their records. While testing could increase treatment options and their potential efficacy for patients who are identified as being at risk or even already affected by life-threatening illness, the awful irony is that early markers could compel insurance companies to deny coverage and thus the funds to pay for expensive treatment, should it become necessary (Harmon 2008). While this not an issue specific to electronic health records and interoperability - it pertains to paper records as well - there seems to be a pervasive anxiety among the general population that recording information electronically and making it potentially accessible to many parties from remote locations constitutes a particularly potent risk.

This fear is even shared by practitioners. In a recent personal discussion, a physician friend speculated that at least half the doctors she knows will not put information on *Synapse*, a "multi-jurisdictional mental health information system" developed collaboratively and used across the country, because of privacy and security concerns, especially when "psych notes" about patients are involved (Spooner 2008), even though the network has been promoted as providing dramatic benefits when it comes to patient care (see Synapse). Perhaps this is because they know how easy it is to access most records. Two additional examples may be illustrative: (1) another friend, a registered nurse also working in Vancouver, lodged a complaint with the hospital in which she worked when it became apparent that co-workers had accessed her medical record and discovered that she had had a miscarriage; (2) my wife (also an R.N.) was easily able to peruse my own medical record when we wanted to quickly view something in my electronic file, even though she was not officially involved in my care. While there may have been an audit trail, she was never contacted about her "unauthorized" access.

Although Canadian patients don't, for the most part, have the same worries about obtaining and retaining health insurance (although for the tens of thousands who travel abroad every year, getting emergency out-of-country coverage may be an issue), there are other considerations. One that is becoming more prominent has to do with finding a family physician when there is a shortage of doctors, such as exists at present. There have been increasing numbers of cases of physician pre-screening of patients; those applicants deemed not to fit the profile that a physician desires in a patient may be rejected. It can be very difficult for some patients to find a doctor willing to accept them (Too sick 2008). Given how simple it appears to be for practitioners to view the records of patients not under their care (based on the anecdotal evidence above), there may be good cause too worry about the expanded circle of potential access offered by widespread integration.

This expanded circle also potentially includes personnel involved in national security, and for Canadians, whose records may end up residing on a U.S. server or with the Canadian subsidiary of a U.S. contractor (as is a possibility in Canada's eHealth program), there is the additional fear of being subject to scrutiny by American law enforcement and intelligence authorities. The Office of the Information and Privacy Commissioner for B.C. has produced an extensive report about the possibility of the private information of Canadians being accessed by U.S. authorities (Office 2004). Among the conclusions is the following: " ... if information is located outside British Columbia, it will be subject to the law that applies where it is found, regardless of an outsourcing contract ... Further ... it is a reasonable possibility that the US Foreign Intelligence Surveillance Court (FISA Court) would issue a FISA order requiring a US-located corporation to produce records held in Canada by its Canadian subsidiary ..." (132).

V. How tight is too tight?

In contrast to the picture painted above, where one might draw the conclusion that security for electronic networks is porous and privacy is in peril, some would take the view that there is *too much* concern about privacy and that existing safeguards are more than adequate - in fact, that they are overly restrictive. In spite of the fact that no fines have been levied in the U.S. with regard to HIPPA law complaints (and there been more than 25,000 complaints to date) (Carroll), there appears to be a wariness about information sharing among some clinics and practitioners that goes beyond prudence and borders on obstruction. In a recent conversation with an anesthesiology resident, I was told by the physician that he had to "constantly wrestle with paraprofessionals to get important information about patients who were in no position to give consent because they were unconscious and in serious condition" (Scott 2008). The doctor wanted data about allergies, medical history and the like, but paraprofessionals connected with the patient's family physician were citing HIPPA in refusing to pass on the critical information. "I would then have to tell them, well, no - HIPPA allows you to give me this information - without the patient's consent - in an emergency situation" (see United States Department of Health and Human Services 2008, for a discussion of the elimination of the consent requirement).

One of the challenges facing practitioners and records managers is sorting out and being clear about what contexts are acceptable for the sharing of health information. This may involve an educational process for individuals within organizations as well as written interpretation (complete with relevant examples) of existing policy and regulations. The rationale for this is as much to ensure efficiency and quality of patient of care as it is to address privacy and security.

Another aspect to consider when discussing stringent privacy rules is the potential dampening effect on research. Putting aside for the moment the fact that "data mining" of patient medical records by large pharmaceutical companies constitutes a contentious issue, related concerns have been raised about the recruitment of patients for institutionally-driven research studies. In B.C., recruitment through the use of government data banks has been suspended since a 2003 amendment to the provincial Freedom of Information and Protection of Privacy Act (FOIPPA) prohibiting release of patient information for the purpose of contacting individuals about participating in research (Fayerman 2008). A variety of studies have been put "on hold," including investigations of cancer by the B.C. Cancer Agency, as well as Parkinson's disease by U.B.C. researchers.

VI. Personal health records

A concept that has been gaining currency in the discussion of medical records and interoperability is that of personal health records or PHRs. AHIMA, while acknowledging that the definition is still evolving defines a PHR as follows:

> The personal health record (PHR) is an electronic, lifelong resource of health information needed by individuals to make health decisions. Individuals own and manage the information in the PHR, which comes from healthcare providers and the individual. The PHR is maintained in a secure and private environment, with the individual determining the rights of access. The PHR does not replace the legal record of any provider" (American 2008).

Already, a number of personal health information repositories have been created, most notably by Microsoft (*HealthVault*), AOL co-founder Steve Cage (*Revolution Health*) and Google (see Mayer 2008, for a preliminary look at *Google Health*). It is clear that these companies have recognized consumer demand for a place they can store - and easily access - personal health information. In some ways, these repositories represent a "sidestepping" or "end run" of the initiatives being promoted by government. A great deal of interest is being shown in PHRs, perhaps because the pace of the drive to standardize and implement interoperability is too slow for some consumers and because accessing personal medical records is still not always easy, or instant, or cheap (most clinics charge money to print patient records) - despite legislation both in Canada and the U.S. promising ready access.

Moreover, the increased control over and greater transparency of medical information offered by the corporate repositories to the patients themselves is appealing to many. Ückert et al. (2004) cite several sources attesting to the value of empowering patients with access to their own medical data. They go on to describe a repository (*akteonline.de*) set up by the Medical Informatics Department at University Hospital Münster, in conjunction with a university spin-off company called Gesakon GmbH. Among other objectives, *akteonline.de* aims to: "give the patient the possibility to manage his own medical data electronically ... incorporate data from different medical applications and systems ... make personalized health care information available to the patient ... serve as a medium for the communication of health care information ... support preventive medical treatment through integrated reminder functions ..." (Ückert et al., p. 2).

Here in Canada, a new initiative by the Canadian Medical Association, called mydoctor.ca, has just been started and promises to give Canadian patients the opportunity to interact with their doctors online, enabling to monitor blood pressure and other conditions, and then checking in with their family physician (Fayerman 2008b).

Issues regarding privacy and security of records are no less pertinent and pressing when it comes to personal health records (*versus* electronic health records residing within an integrated national system) (Reed 2008). Nevertheless, patients availing themselves of the PHR repositories would appear to be willing to accept the risks, given perceived advantages regarding access and empowerment. Certainly, given the millions of persons (many of them elderly) spending significant amounts of time every year in foreign locales (sometimes engaging in "medical tourism" - see Shirley 2008, for example), compelling arguments can be made for having transnational PHR storehouses that are not as encumbered by privacy legislation so as to be dysfunctional.

Of course, when it comes to producing records that can be used in legal circumstances as evidence, it is doubtful that any record that could be easily altered or edited by a patient would be considered acceptable. This implies that PHRs cannot replace an “official” system of EHRs - the suggestion is that dual (or parallel) systems would be needed - one for the patients (with easy access and editing possibilities) and another for evidentiary purposes. On the face of it, this would seem to be an expensive prospect, with practitioners having to “double report” while coordinating what information was going into what systems.

VII. Conclusion

This paper has attempted to paint - in very broad strokes - some of the central issues and concerns residing prominently in the foreground of the rapidly changing medical records landscape.

Although there are some challenging technical issues for records managers regarding coding and standardization, in the end, the key problems concerning interoperability with regard to medical records can be rendered down to the question of how to reconcile improved access with adequate privacy. At stake are enormous potential benefits with regard to patient safety and quality of care. In the U.S it is estimated that up to 98,000 lives may be saved per annum and an 80% improvement in recommended care could be realized, if preventable medical errors - most of which are due to erroneous or missing information - can be eliminated (Commission, vi). Also worth mentioning is the ongoing benefit to patients who are properly attended to from the start and who will not suffer the continuing effects resulting from medical errors committed early in the cycle of their care. The financial benefits to be gained from increased efficiency in the U.S. alone are estimated to be in the hundreds of billions of dollars annually (vi).

Also at stake, however, are the potentially devastating (to some) consequences of the improper disclosure or inadequate protection of personal health information. Jobs, affordable care, or even regular, consistent access to a family doctor may hang in the balance.

A corollary question for policy makers and records managers, then, concerns whether a trade-off is, in fact, inevitable when it comes to access and privacy. Can we ever ensure that privacy will not and cannot be breached 100% of the time? If perfection is deemed unattainable, the challenge for politicians and information managers will be to decide what balance is acceptable and how to continue to make any compromise less onerous.

Works Cited

Akteonline.de (2008) [Internet website], Gesakon GmbH. Available from: <https://www.akteonline.de/> [Accessed: 17 March 2008].

Alvarez, R. (2005) Health care has to move into the hi-tech age. *Bulletin of the World Health Organization*, 83 (5) May, p. 323. Available from: <http://www.who.int/bulletin/volumes/83/5/editorial20505html/en/> [Accessed 6 March 2008].

American Health Information Management Association (2007) *Statement on consistency of healthcare diagnostic and procedural coding* [Internet], AHIMA, December. Available from: <http://www.ahima.org/dc/positions/documents/MicrosoftWord-ConsistencyofHealthcareDIagnosticandProceduralCoding-appv12-1-2007.pdf> [Accessed 17 March 2008].

American Health Information Management Association (2008) Personal health records [Internet], AHIMA. Available from: <http://www.ahima.org/emerging%5Fissues/PHR.asp> [Accessed 17 March 2008].

A new era in interoperability. (2007) *E-health Insider* [Internet], 27 September. Available from: <http://www.e-health-insider.com/Features/item.cfm?docID=212> [Accessed 9 March 2008].

Buckler, G. (2008) Health records: Canada lags in electronic medical records [Internet], *CBC News*. 28 January. Available from: <http://www.cbc.ca/news/background/healthcare/records.html> [Accessed 6 March 2008].

Canada Health Infoway (2008) *Infoway: Establishing electronic health records for Canadians – who we are* [Internet], Canada Health Infoway. Available from: <http://www.infoway-inforoute.ca/en/WhoWeAre/Overview.aspx> [Accessed 17 March 2008].

Canadian Medical Association (1998) *CMA Health Information Privacy Code* [Internet], 15 August. cma.ca. Available from: <http://www.cma.ca/index.cfm/ci_id/3216/la_id/1.htm> [Accessed 17 March 2008].

Carroll, J. (2007) Privacy concerns delay health information network. *Managed Care*, 16 (4) April, pp. 8, 13. Available from: <http://www.managedcaremag.com/archives/0704/0704.regulation.html> [Accessed 9 March 2008].

Collins, T. (2007) Security warning as NHS staff view celebrity record *ComputerWeekly.com* [Internet], 17 September. Available from: <http://www.computerweekly.com/Articles/2007/09/17/226792/security-warning-as-nhs-staff-view-celebrity-record.htm> [Accessed 9 March 2008].

Commission on Systemic Interoperability (2005) *Ending the document game: Connecting and transforming your healthcare through information technology* [Internet], Washington, U.S. Department of Health and Human Services (HHS). Available from: <http://endingthedocumentgame.gov/PDFs/entireReport.pdf> [Accessed 9 March 2008].

Craig, B. (1990) Hospital records and record-keeping, c. 1850-c. 1950. Part I: The development of records in hospitals. *Archivaria*, 29 Winter 1989-1990, pp.57-67.

Fayerman, P. (2008) Privacy law freezes health research. *Vancouver Sun*, 9 January, pp. A1-2.

Fayerman, P. (2008b) Now you can visit your doctor online. *Vancouver Sun*, 2 April, pp. A1, 5.

Foundation for eHealth (2008) *eHealth Initiative – About* [Internet], Available from: <http://www.ehealthinitiative.org/about/mission.mspx> [Accessed 17 March 2008].

Geltzer, R. (2008) Metadata, law, and the real world: Slowly, the three are merging. *Journal of AHIMA*, 79 (2) February, pp. 56-57, 64.

Greiver, M. (2008) *Dr. Greiver's EMR* [Internet web log], Available from: <http://drgreiver.blogspot.com/> [Accessed 6 March 2008].

Harmon, A. (2008) Fear of insurance trouble leads many to shun or hide DNA tests. *New York Times,* 24 February, pp. 1, 19.

HealthVault (2008) [Internet website], Microsoft Corporation. Available from: <http://www.healthvault.com/> [Accessed 17 March 2008].

Heubusch, K. (2006) Interoperability: What it means, why it matters. *Journal of AHIMA*, 77 (1) January, pp. 26-30. Available from: <http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_028957.hcsp?dDocName=bok1_028957> [Accessed 17 March 2008].

Mayer, M. (2008) Google Health, a first look [Internet blog], *The Official Google Blog*. Available from: <http://googleblog.blogspot.com/2008/02/google-health-first-look.html> [Accessed 17 March 2008].

Office of the Information and Privacy Commissioner for B.C. (2004) *Privacy and the USA Patriot Act* [Internet], Victoria, Office of the Information and Privacy Commissioner for B.C. Available from: <http://www.oipcbc.org/sector_public/archives/usa_patriot_act/pdfs/report/privacy-final.pdf> [Accessed 15 March 2008].

Office of the Privacy Commissioner of Canada. (2004) *Health links – Privacy Commissioner of Canada* [Internet], Ottawa, Office of the Privacy Commissioner of Canada. Available from: <http://www.privcom.gc.ca/information/02_03_02_e.asp> [Accessed 15 March 2008].

Personal Information Protection and Electronic Documents Act 2000, c.5 (2008) Department of Justice Canada [Internet], 10 March. Available from: <http://laws.justice.gc.ca/en/P-8.6/text.html> [Accessed 17 March 2008].

Pickard, B. (2007) *Testimony of Bryon Pickard, MBA, RHIA, President American Health Information Management Association to the Committee on Oversight and Government Reform, Subcommittee on Information Policy, Census and National Archives* [Internet], 10 July. Available from: <http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_034565.pdf#xml=http://library.ahima.org/xpedio/idc> [Accessed 17 March 2008].

Reed, T. (2008) Google tries to calm fears over privacy of health service. *MercuryNews.com* [Internet], 29 February. Available from: <http://www.mercurynews.com/ci_8403736?source=rss&nclick_check=1> [Accessed 16 March 2008].

Revolution Health (2008) [Internet website], Revolution Health Group, LLC. Available from: <http://www.revolutionhealth.com/> [Accessed: 17 March 2008].

Rhodes, H. (2006) Privacy and security challenges in HIEs: Unique factors add new complexities to familiar issues. *Journal of AHIMA*, 77 (7) July/August, pp. 70-71, 74. Available from: <http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_031662.hcsp?dDocName=bok1_031662> [Accessed 17 March 2008].

Savvas, A. (2008) Stockport Primary Care Trust loses 4,000 patient records on memory stick. *ComputerWeekly.com* [Internet], 18 January. Available from: <http://www.computerweekly.com/Articles/2008/01/18/228990/stockport-primary-care-trust-loses-4000-patient-records-on-memory.htm> [Accessed 9 March 2008].

Scott, T. (2008) [Personal interview], 23 February.

Shirley, R. (2008) A trip to the dentist - Argentina style. *Vancouver Sun,* 15 March, p. G6.

Spooner, L. (2008) [Telephone interview], 3 February.

Synapse (2002) *Synapse overview – benefits* [Internet], Synapse.com. Available from: <http://www.synapse-ehr.com/synapse_overview/benefits.htm> [Accessed 17 March 2008].

Too sick to be a patient, Winnipeg woman told. (2008) *CBC News* [Internet], 23 January. Available from: <http://www.cbc.ca/health/story/2008/01/23/doctor-rejection.html> [Accessed 6 March 2008].

Ückert, F., M. Müller, T. Bürkle, and H. Prokosch (2004) An electronic health record to support patients and institutions of the health care system [Internet], *German Medical Science*, 2 (Doc06) (provisional PDF). Available from: <http://www.egms.de/pdf/gms/2004-2/000016.pdf>.

United States Department of Health and Human Services (2008), Why was the consent requirement eliminated from the HIPPA Privacy Rule, and how will it affect individuals' privacy protections? [Internet], HHS. Available from: <http://www.hhs.gov/hipaafaq/about/193.html> [Accessed 17 March 2008].

United States Department of Health and Human Services, Office for Civil Rights (2008) *HHS - Office for Civil Rights - HIPPA* [Internet], HHS. 30 January. Available from: <http://www.hhs.gov/ocr/hipaa/> [Accessed 17 March 2008].

Additional Relevant Resources

American Medical Informatics Association (AMIA)
http://www.amia.org/

AMIA/AHIMA (2007): *Healthcare terminologies and classifications: Essential keys to interoperability* [a white paper]
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_034273.pdf

Canadian Health Information Management Association (CHIMA)
http://www.echima.ca/pages/01about/01about_us.html

Canadian Institute for Health Information (CIHI)
http://secure.cihi.ca/cihiweb/dispPage.jsp?cw_page=home_e

Health Canada – eHealth
http://www.hc-sc.gc.ca/hcs-sss/ehealth-esante/index_e.html

International Council on Medical & Care Compunetics (ICMCC):
Interoperability articles:
http://articles.icmcc.org/wpc/tag/interoperability
Electronic Health Record (EHR) articles:
http://articles.icmcc.org/wpc/?cat=7

The Medical Librarian (blog)
http://themedicallibrarian.blogspot.com