Privacy of Electronic Health Records: Public Opinion and Practicalities

Michael Smit
Faculty of Computer Science
Dalhousie University
Halifax, Nova Sotia
Email: smit@cs.dal.ca

Michael McAllister
Faculty of Computer Science
Dalhousie University
Halifax, Nova Sotia
Email: mcallist@cs.dal.ca

Jacob Slonim
Faculty of Computer Science
Dalhousie University
Halifax, Nova Sotia
Email: slonim@cs.dal.ca

Abstract

Governments and healthcare providers are moving to electronic health records (EHRs) to lower the cost of healthcare, improve patient care, and reduce medical errors. A critical issue in the transition to EHRs is the privacy, confidentiality, and security of the information stored. This issue has made some patients and healthcare providers reluctant to accept electronic records. To begin to address this issue and spur the adoption of EHRs, we examine the views of the general public regarding personal health information and the implications of electronic health records. Based on public opinion and the practicalities of storing and controlling personal information, we conclude that individuals must have control of their personal health information, but that a non-governmental third-party organization not involved with healthcare is the entity best-suited to encourage patient trust and ultimately allow for the widespread public acceptance of electronic medical records. We suggest a transaction management model that would enable such an entity to implement individualized control of personal information.

1 Introduction

The proper management of personal health information is important to the healthcare system. Patients share this information with their physician in the expectation it will be used to improve their health and comfort. The physician adds information regarding his or her diagnosis and treatment of the patient. Information is also generated by laboratories, pharmacies, hospitals, and other healthcare stakeholders. In totality, this information comprises the patient's health record, which may be segmented in physically separate locations under the custodianship of several different healthcare providers.

For the most part, this process happens on paper: approximately 80% of Canadian doctors, clinics, and hospitals use paper records [11], and 90% of health-related transactions in the United States are completed on paper [28]. This largely paper-based administration accounts for 16.7% of all healthcare expenditures in Canada, and for 31% in the US (roughly $300 billion USD) [39]. Many stakeholders in the healthcare system see electronic health records as a way to improve the quality of care while decreasing costs. The government and key healthcare stakeholders in both countries are pushing for a change from paper to electronic health records (EHRs). Canada Health Infoway [6] has been commissioned to design a national electronic health record infrastructure and work with Health Canada and provincial health departments to begin the deployment of this infrastructure. In the US, the President used the State of the Union address to announce a plan that ensures most Americans have electronic health records within the next decade [37].

As we make this transition from paper to electronic records, it is critical that we address the privacy, confidentiality, security, and trust issues that will arise. Doctors, patients, and other healthcare stakeholders agree that the benefits of electronic health records cannot come at the cost of confidentiality of personal health information. However, computer scientists and other technical people do not always see the perspective of those who will be the most affected by a move to electronic records. Thus, on behalf of the Canadian Medical Association (CMA), we undertook a comprehensive literature review to assess public opinion (and the opinions of other healthcare stakeholders) regarding any health information-related issue. This paper shares some of the public opinion data that we found, and presents some of the conclusions that we reached based on this information.

We begin by examining why and how trust is important to healthcare and addressing public and physician perspectives on trust, personal health information, and the implications of moving to electronic health records. We then discuss methods to increase trust in the proper handling of personal information. Based on these results, we discuss the practicalities of storing and controlling personal health information, proposing that a third-party with nothing to gain from having access to personal health information provide a data warehouse service. We conclude by proposing one tool to help meet the stringent privacy and data protection requirements inherent to electronic health records: a token-based distributed transaction model.

2 Definitions

When discussing topics related to privacy, different organizations will use slightly different definitions of the terms (e.g., [1, 2, 9, 17, 33]). In general, definitions include informed consent and the right to make decisions about how one's own information is used. For a definition of privacy within the context of healthcare, we turn to the Canadian Medical Association: "...a patient's right to determine with whom he or she will share information and to know of and exercise control over use, disclosure and access concerning any information collected about him or her; it entails the right of consent" [7].

Although However, it is important to be aware of the terminology differences when examining the results of studies conducted by these different organizations. In particular, the general public does not have a precise definition of any of these terms. As we see it, the notion of privacy when discussed by the general public often encompasses far more than the academic definition of privacy. Many survey results will reflect the public's opinion of a combination of privacy, confidentiality, and security. Therefore, we will use the term 'privacy' in the same general way, unless specified otherwise. While less precise, this practice is consistent with the data available.

3 The Importance of Privacy and Trust to Healthcare

Individuals consider their personally identifiable health information to be private - they have a right to decide who gets to see it, and once they reveal it to that party, they expect it to remain confidential. Most rank it as being the most sensitive personal information, along with financial information [15, 18, 19, 36]. If patients are not able to trust that their personal health information will be adequately protected by the health record system that stores it, they may not fully participate in their healthcare. They may not completely reveal information that is sensitive, even though it is important to their care [16].

In Canada, surveys show that 11-13% of Canadians have held back information from a health provider because they were afraid of who would see it and for what it would be used [3, 8]. A 1999 survey of American citizens found that 15% of individuals were taking action to keep their personal medical information private by not seeking treatment, 'doctor-hopping', paying out of pocket, giving inaccurate or incomplete information, or asking their doctor to keep information out of their record [32]. A 2005 survey of Americans found that 65% were very or somewhat concerned that "people will not disclose sensitive but necessary information to doctors and other health care providers because of worries that it will go into computerized records" [22][1].

There are some privacy concerns even about paper records; it seems that some individuals do not want their health information recorded in

[1] The question did not ask if the respondent would personally refrain from disclosing personal information; rather, it asked if the respondent was concerned about other people not disclosing their own information.

any format. Although it is difficult to directly compare public opinion on this issue, the numbers suggest that more individuals have concerns when the format is electronic. If these concerns are not resolved before the widespread introduction of electronic health records, people will not trust EHRs enough to reveal sensitive information, or to allow their doctor to record this sensitive information. This will be detrimental to the quality of care the patient receives and to the ability of other stakeholders to do their jobs.

It is in the best interests of everyone involved (the patient, clinicians, researchers...) to have accurate and complete information. Patients have a high level of trust for their family physician, which gives them the comfort necessary to reveal personal and sensitive information [27]. However, if both the patient and the doctor have misgivings about electronic health records, all of the patient's information might not be stored in the record. A 2001 poll of doctors conducted by the Association of American Physicians and Surgeons (AAPS) found that 87% of doctors had a patient who had asked them to withhold information from their medical record. The same poll found that 78% of doctors had withheld information due to a patient's "privacy concerns" [5].

4 Trust within the Healthcare System

Physicians receive high trust ratings (above 90%) from the general public when it comes to "doing the right thing" for a patient and/or a patient's healthcare, and when it comes to telling the truth [15, 20, 21, 29, 30]. In a 2000 Canadian poll, nurses, pharmacists, and doctors were trusted by over 90% of respondents when compared to other professions such as judges and civil servants (Fig. 1) [30]. When asked about personal health information in particular, 75-80% of Canadians polled felt that the information they gave their physician was kept confidential. Over 17% felt that this information was not kept confidential [3, 8].

There are differing levels of trust for different stakeholders in health care. While 96% of Americans trusted their doctor to "do the right thing" for them and their healthcare, only 54% feel the same about their managed care company (Fig. 2) [21]. Focus groups in the UK felt that their physician should have unrestricted access, that specialists and surgeons should have limited access based on the context, and that office receptionists should not have access at all [12]. A Gallup poll conducted in 2000 found that Americans had strong opposition to non-medical groups seeing their medical records [15] (see Fig. 3), with the government being the group least likely to be granted access. This mistrust extended to agencies controlled by the government; a Canadian provincial survey found that only 33% agreed with that all health information should be controlled by a central agency responsible to the government [36].

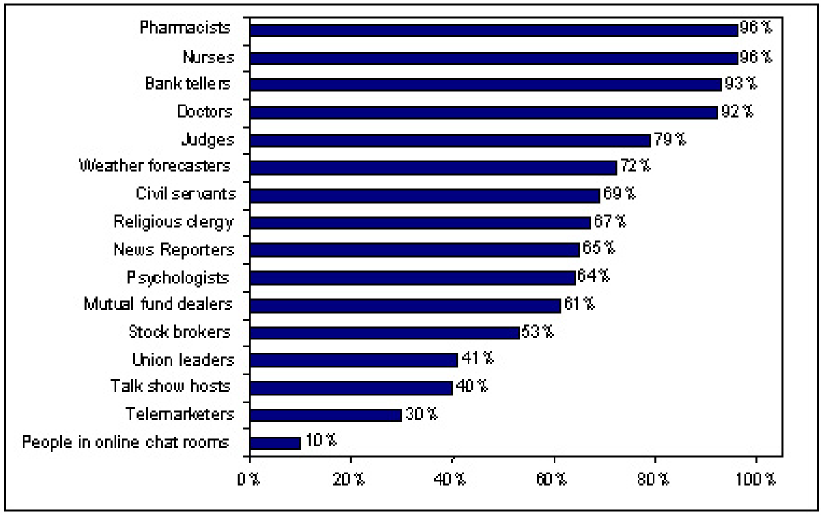

Figure 1: Trust Canadians expressed for selected professions [30]

It appears that patients make determinations on who they trust with their information based on the potential trustee's role and the context of the situation. Their trust for healthcare professionals with whom they have firsthand contact is high. Those who are professionals but do not have contact with the patient - specialists, researchers, and the like - are trusted less, and administrators are trusted least of all (perhaps because there are fewer professional codes of conduct for healthcare administrators).

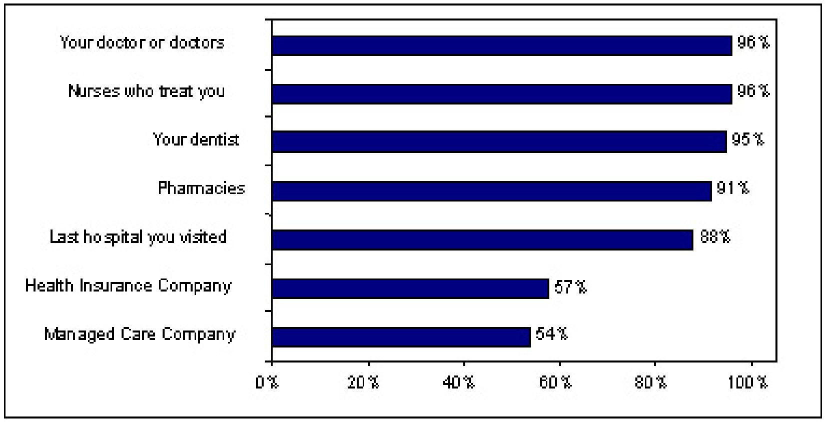

Figure 2: Trust Americans expressed for various health-related professions [21]

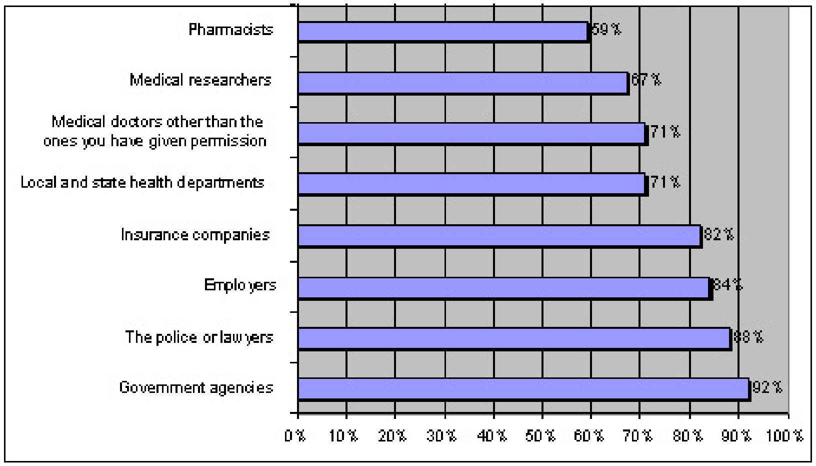

Figure 3: Americans opposed to allowing group to see medical records without permission [15]

When considering electronic health records in particular, more than half of American citizens polled in 1999 felt that a move from paper to electronic records would make it "more difficult to keep personal medical information private and confidential" [32]. An Albertan study found that 82% of Albertans felt it was appropriate to place patient information in an electronic record (with the condition that they could control who has access to the record). When asked to pick their number one concern about electronic health records, the majority were concerned with inappropriate access to their information (Fig. 4) [18]. Nationwide, 66% of Canadians agree electronic health records should be implemented to "improve the integration of services and monitor the use of many health care resources, even if this means that the records will be accessible by other health care providers" [31].

A 2005 Harris telephone poll of Americans [22] found that 71% had not heard that the White House was actively calling for a nationwide program for electronic health records. After being informed about the project and the definition of an EHR, respondents were asked to gauge their level of concern regarding about some of the potential negative impacts of EHRs. Approximately 70% were concerned about data leaks, medical information being shared without their knowledge, poor security, and increased medical errors. The full results are in Table 1. The poll is not clear on whether they were concerned that this would happen, or whether they would be concerned if it did happen. It also did not distinguish between asking if the respondent would personally behave in a certain way or if they were afraid that other people would behave a certain way.

The same survey [22] found Americans were split on whether the potential benefits of electronic health records outweighed the risks - 48% said that the "expected benefits outweigh the risks to privacy", and 47% said that the "privacy risks outweigh the expected benefits."

An unrelated Harris poll of online Americans [23] found that 76% of those polled believe that electronic medical records will improve their medical care, 73% believe it would reduce health care costs, and 63% believe it will reduce the frequency of medical errors. After acknowledging these benefits, 67% said they believe that electronic health records would make it more difficult to ensure patient privacy [23]. Some of these numbers, most notably the 63% who believe EHRs will reduce

-	-	Very Concerned	Somewhat Concerned	Not Very Concerned	Not at all Concerned	Not Sure
Sensitive personal medical-record information might be leaked because of weak data security	%	38	32	16	13	1
There could be more sharing of your medical information without your knowledge	%	42	27	18	13	–
Strong enough data security will not be installed in the new computer system	%	34	35	18	12	1
Some people will not disclose sensitive but necessary information to doctors and other health care providers because of worries that it will go into computerized records	%	29	36	20	13	1
Computerization could increase rather than decrease medical errors	%	29	36	22	13	1

Table 1: Concerns individuals have about electronic health records [22].

the frequency of errors, directly contradict the other Harris report we discuss above [22]. Harris has offered no explanation for this difference. One difference is the questions asked: the first poll prefaced each potential concern with this statement: "Here are some things that some people have said might happen under such a patient Electronic Medical Record system. How concerned are you that...?" The second poll prefaced the question with this statement: "How strongly do you agree or disagree with each of the following statements?". Despite these differences, in both polls the percentage who were concerned about the difficulties involved in protecting patient privacy are near 70%.

Some proposals for EHR systems include the use of unique identifiers that are assigned to each patient and associated with their entire medical record. A Princeton Research Associates poll conducted in 2000 found that when told about the potential benefits as well as the risks in adopting a system of unique identifiers, 39% of Americans favor health identifiers while 52% are opposed. The survey also asked how concerned respondents were about various potential risks of unique health identifiers (Fig. 5). According to the researchers, "The survey results confirm that medical privacy concerns currently play an important role in limiting public support for unique health identifiers" [32].

There are certainly concerns about the protection of personal health information stored in electronic health records. Many are concerned about authorized users abusing their access rights to access information that they should not. Another common concern is attackers from outside attempting to gain access. An EHR system needs to assure users that it can adequately protect their information. It also seems that the average individual is not well-informed about the basics of EHRs. The public may require extensive education regarding the benefits (and

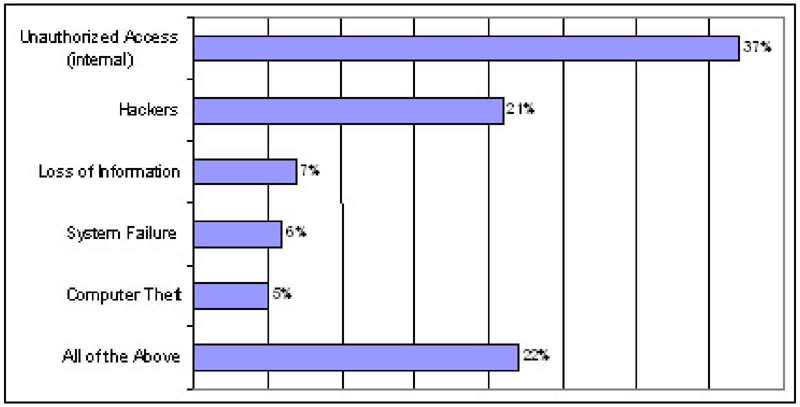

Figure 4: First place rankings for concerns about Electronic Health Records [18]

risks) of EHRs prior to their widespread adoption.

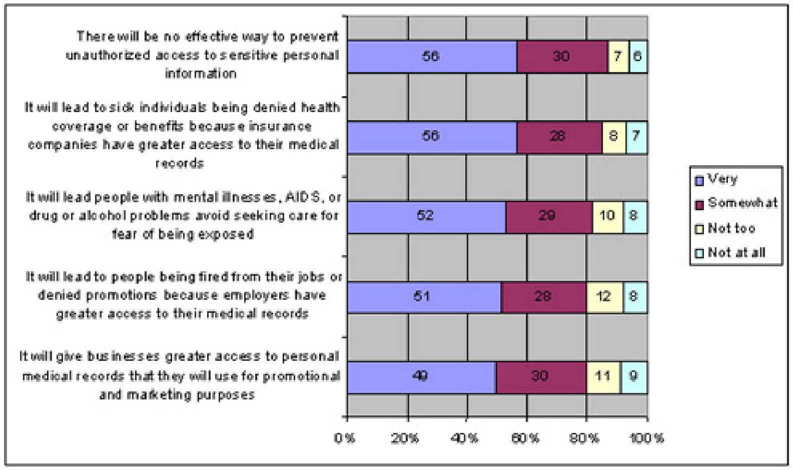

Figure 5: Percentage of Americans concerned about potential risks of health identifiers [32]

5 Physicians and Health Records

There is little statistical data available on physician opinion regarding confidentiality. However, we present results from the COMPETE[2] study, which conducted one-on-one interviews with physicians:

> "There was considerable concern over the burden of asking their patients for consent to use their personal health information for research purposes. Physicians question whether they or their patients could adequately articulate the issues involved in this kind of research to obtain a valid consent."
>
> "There is a large onus on the physician both to understand the risks and benefits of the research and to convey those adequately to the patient - a task which physicians themselves, in phase 1, felt they could not adequately do under current circumstances."
>
> "Many stated they wanted to be 'on the side' of the patient on privacy issues. However, there was disagreement on ownership and control of use of anonymized patient records, with some having no difficulty with disclosure of anonymous information and others opposed." [38]

An AAPS poll [5] found that "nearly 87% [of responding physicians] reported that a patient had asked that information be kept out of the record, and nearly 78% said that they had indeed withheld information from a patient's record due to privacy concerns. While only 19% admit to lying to protect a patient's privacy, 74% state that they have withheld information for that reason."

[2] Computerization of Medical Practices for the Enhancement of Therapeutic Effectiveness. The project "...assessed concerns over the use of information from electronic medical records for research and preferences for consent of patients whose doctors were enrolled in a southern Ontario project to improve prescribing through the use of electronic medical records..." [38]

6 Encouraging Trust

Given the importance of trust to the healthcare system, it is important that patients, physicians, and other healthcare stakeholders trust the electronic health record system that is adopted.

Many theoretical models have been built to predict or understand consumer trust in the setting of electronic commerce (see, for example, [4, 13, 24–26, 35]). There are also more general methods suggested to develop trust, such as those espoused by Doney et. al. [14]. Doney believes, in brief, that individuals can build trust based on endorsement from a trusted third party, favourable analysis of a potential trusee's motives, confidence in the trustee's ability to keep their promises, recollection of past behavior, or attempting to guess the cost-benefit analysis a trustee is using. From this, we could surmise that an electronic health record system must receive the support of physicians and other trusted healthcare stakeholders, and that these records must be physically stored by an entity that has manageable motives, has the resources required to design and maintaing a secure data storage system, has performed well in the past, and has a strong reputation.

However, there are not enough large-scale surveys to prove this true for health care records. There is little literature presenting actual public opinion on what it takes for them to trust an entity in the electronic realm.

An Australian study [34] asked respondents to name ways an organization could build trust with its customers. The largest block of respondents (60%) said their trust was correlated with how much actual control they had over how their personal infromation was used. Other respondes included visible and understandable privacy policies, good past experience, good reputation, and staff showing respect for privacy.

A province-wide study in Saskatchewan [36] found that over 90% of patients 'felt strongly' that personal health information should only be disclosed with their consent. The same study, as well as an unrelated study in Alberta, [18] found that when asked, over 70% of people favour a law specifically aimed at protecting health information, and some provinces have passed or are creating laws designed to protection the confidentiality of health information. It is this 'consent', or 'control', that can be difficult to practically achieve using paper records. A clear benefit of electronic health records is the potential to have access to and use of the health record under the direct control of the patient, if they request it.

7 Storing Electronic Health Records – Ideals vs. Practicality

We began by discussing public opinions of privacy, and most agree that the owner – if not always the custodian – of health information is the patient. However, security and privacy are not necessarily issues for which we should ask for a show of hands. The average individual does not have the technical knowledge to make informed decisions about how best to protect electronic health records. While each individual could store their own records (on a smart card, for example), this reduces the availability of the information. In an emergency, we can not rely on individuals to produce their own health records, especially in cases of acute care for life-threatening injuries. There must also be some backup location to maintain the information in case the card is lost or stolen, so the patient will actually have control of only one copy of their records, while another copy is controlled by others. Giving a patient a smart card with their personal health information may provide the feeling of control, but this control would be an illusion - the master copy of their information would be elsewhere and controlled by others.

The custodianship of personal health information has always been a task most patients have been comfortable leaving in the hands of a trusted professional, most often their family doctor. Doctors have generally been comfortable in this role, which they take very seriously. However, with the advent of electronic records, it is impractical to ask each general practitioner to develope, maintain and protect an electronic health record system. They will not have the resources to hire a full-time administrator, nor will they have the time or expertise to deal with the system in-house. Developing the security protections necessary to maintain patient confidentiality and guard against and monitor external breaches is a daunting task. Deploying these measures, or hiring and paying staff to deploy these measures, is not efficient use of a primary care provider's time.

Allowing patients to store their own information is one way to ensure that they have control. Another way is to allow the physician to store the records, act as custodian, and take guidance regarding the handling of the records from the patient. However, these solutions are not ideal in the real world. Thus, we consider a solution where the records are stored by a trusted third-party, but access to these records is controlled completely by the patient. This third party will be contractually or legally bound to grant an entity access to an individual's personal information only when permitted by the individual. With such a system, the patient can control their personal health information without worrying about logistical details like security, encryption, or immediate access to the information in emergencies. The third party provides a service; it is essentially a storage medium. The patient dictates when and to whom information is released.

The remaining question concerns the nature of this third-party. Many organizations have enumerated requirements for electronic health record systems. They must be available in times of emergency; those who store records must be accountable; the security of records, both internally and externally, must be assured; patients must have access to their own records; the data must be accurate; the integrity of the data must be assured; and finally any user preferences must be easily understood by those required to set them. To this list we would add:

1. *Individuality.* The system should be capable of representing a patient's personal privacy preferences, and adhering to them. Privacy and confidentiality are areas where personal differences of opinion abound.

2. *Dynamic.* Patient privacy preferences are not static; they are ever-changing, always adapting to context, experiences, media coverage, and any number of other factors. Many patients have different levels of trust for different areas of the healthcare system [21]. A system needs to be capable of representing these preferences with sufficient detail.

What type of organization is capable of meeting these requirements? One suggestion is a government agency. Governments around the world are already significantly invested in healthcare; it may seem natural for them to take on the role of storing information as well. Many government agencies already use and store personal health information - deidentified or otherwise. However, the Gallup poll [15] referenced earlier in Figure 3 shows that 92% of Americans are uncomfortable granting governments access to their personal information. We will rely on the laws of the land to hold the entity storing personal information accountable; allowing the lawmakers to be this entity may represent a conflict of interest. More worrisome is the possibility that governments could begin to combine health information with the already significant amount of personal information they store. These concerns and others leave stakeholders concerned about storing personal health information with government agencies.

Another possibility is insurance companies or managed care companies. These businesses stand to benefit financially from a switch to electronic records - they currently pay a significant portion of the administration costs electronic records are designed to reduce. However, these companies are often the least trusted of all healthcare stakeholders [21]. Patients see them as having a vested interest in their own profits, putting a higher priority on the bottom line than on individual privacy. It is difficult to inspire trust in the secure and private storage of health records when the data storage entity is known to have a vested interest in the contents of these records.

This leaves us with third-party, non-governmental entities that are not part of the healthcare system. In this case, we are trading the pre-existing trust many individuals have for healthcare organizations for the trust that comes from knowing an entity has nothing to gain by misusing the records [14]. This third-party must have the experience and capability to securely and privately store personal information. Data warehousing is not a new idea; many organizations have experience using or providing such a service. These organizations must be compelled to protect the confidentiality of these records, and must be able to commit significant resources toward achieving this goal.

Recently, there have been a number of news stories in North America regarding the mishandling of individual information. If we consult public opinion on third-party organizations, surveys show that some individuals do not trust entities that store or collect personal information. They believe these entities lack the expertise or appropriate policies to protect information from unauthorized access, they fear that the policies set may be violated, and they feel that privacy is not considered important. However, these surveys also show that this trust could be established by openness about information handling procedures, by laws with proper enforcement, by a proven track record or a recommendation, and by third-party audits of information handling practices. If these steps are implemented, and if in addition this third-party only stands to gain if the information is protected, and only stands to lose otherwise, then the necessary trust can be established.

The health information system is by its nature distributed - health information is gathered at many locations, and can be accessed from many locations. Proposing that a single entity responsible for information storage does not prohibit a distributed architecture. The database transaction manager we discuss below can help transfer informations securely and privately over a distributed database.

8 Token-passing Peer-to-peer Interaction Coordination

We suggest that the third-party entity implement their security using an architecture proposed in a PhD thesis by Theodore Chiasson [10]. The protocol, called token-passing peer-to-peer interaction coordination (TPIC), allows distributed users and data warehouses to transfer information to/from those who need/store it without requiring any knowledge of global state, database architecture, or even implementation details. Traditional distributed database architectures require that each entity involved in a transaction have knowledge of the global state. However, if all of the participants in a transaction are not trusted equally, patients may not wish to entrust their private health information to a system where every participant has global knowledge. At the same time, the database needs to guarantee the ACID properties. Regarding atomicity, we need a method to ensure that the elements of a transaction either all abort or all commit without using any global knowledge.

Chiasson's solution treats each participant in the transaction as a single peer in a peer-to-peer network. Each peer has its own self-contained database management system (DBMS) used to store information particular to that peer. A set of long-term contracts between peers governs the transaction and how it proceeds. It also provides the information each peer needs to access or modify information contained in the database of another peer (where there is a contract between those two peers). The participant that begins a transaction is termed the *originating peer*. This peer generates a token that contains encrypted information needed for the transaction, a path from peer to peer, a list of transactions to execute at each peer (termed *microtransactions*), and the appropriate logs. This token follows the path, stopping at each peer to allow the local processing layer to load temporary tables, execute microtransactions, make appropriate modifications to its permanent tables, and copy the results back to the token. When the token returns to the originating peer for the final time, all data is returned to permanent tables and the transaction is marked as complete.

The DBMS at each peer is not aware that it is part of a larger transaction; it treats the microstransactions like it would any other transaction. Thus, local recovery is handled completely by the local DBMS. However, should a microtransaction abort at some point along the token path, all of the peers encountered thus far will have modified their databases according to the token plan. Such a failed token is returned to the originating peer. The log of the failed token is used to generate a new token, containing *compensating microtransactions* that will nullify the modifications made based on the microtransactions included on the original token. Recovery for lost tokens and other failure cases is handled in a similar manner.

The information transported on the token - and other potentially sensitive information, such as microtransactions, is encrypted using keys stored in the contracts. There need only be one copy of sensitive information, and it can be used by many peers without ever being permanently stored in their database. Each party that has access to private information is contractually bound to use the information in the way agreed upon by the owner of the information in the contract.

We are developing a prototypical implementation of TPIC as proof-of-concept.

9 Conclusion

As healthcare leaders begin or continue the transition from paper to electronic records, we conclude that attaining and maintaining the trust of patients and the other stakeholders is crucial to their success. We have presented public opinion information from patients and other healthcare stakeholders that shows that medical privacy is important. Patients have varying degrees of trust for other stakeholders, although this trust can be increased using appropriate methods.

Based on our discussion of the practicalities involved with various organizations storing / controlling personal health information, we conclude that a non-governmental third-party with no current stake in the healthcare system is the best practical choice for a data warehousing provider. Although there may be some initial concern about entrusting sensitive information to 'outsiders', we conclude it is necessary to overcome the privacy and security roadblock and achieve the trust needed for EHRs to be widely adopted. The government and various healthcare stakeholders will set the policies that govern the management of this information, and the patient will have ultimate control over their personal information, but a third-party should be the service provider that enforces the access policies that are set. We also propose that this provider use a model similar to TPIC to help ensure confidentiality when working with this sensitive information.

Electronic health records hold enormous potential for improving treatment while decreasing cost. However, the implications of readily accessible sensitive information stored electronically must be examined – and dealt with – before we move to a large-scale deployment. We have used public opinion to motivate our recommendation that we look to an 'outside' third party to ensure the privacy and confidentiality of personal health information.

References

[1] *Oxford English Dictionary*, 2nd ed. OED Online. Oxford University Press, 1989.

[2] American Medical Association. Protecting identifiable health care informational privacy, 2000.

[3] Angus Reid. National Angus Reid omnibus survey for the Canadian Medical Association, 1998.

[4] Araujo, I., and Araujo, I. Developing trust in internet commerce. In *the Conference of the Centre for Advanced Studies on Collaborative research* (2003), pp. 1–15.

[5] Association of American Physicians and Surgeons. New poll: Doctors lie to protect patient privacy, 2001.

[6] Canada Health Infoway. http://www.infoway-inforoute.ca/.

[7] Canadian Medical Association. Health information privacy code, 1998.

[8] Canadian Medical Association. Press release: Canadians highly value the privacy and confidentiality of their health information, 1999.

[9] CANARIE Inc. Ensuring privacy and confidentiality on Canada's Health Iway, 1997.

[10] Chiasson, T. *Token-based Peer-to-Peer Interation Coordination.* Phd, Dalhousie University, 2003.

[11] College of Family Physicians of Canada. National family physician workforce survey, 2001.

[12] Cushnahan, C. Public views on the sharing of personal and medical and social care information, 2000.

[13] da Chen, L., Gillenson, M. L., and Sherrell, D. L. Consumer acceptance of virtual stores: a theoretical model and critical success factors for virtual stores. *ACM SIGMIS Database 35*, 2 (2004).

[14] Doney, P., Cannon, J., and Mullen, M. Understanding the influence of national culture on the development of trust. *Academy of Management Review 23*, 3 (1998), 601–620.

[15] Gallup Organization. Public attitudes toward medical privacy, 2000.

[16] Goldman, J. Protecting privacy to improve health care. *Health Affairs 17*, 6 (1998), 47–60.

[17] Goldman, J., and Mulligan, D. Privacy and health information systems: A guide to protecting patient confidentiality, 1996.

[18] GPC Alberta. Oipc stakeholder survey 2003 - highlights report, 2003.

[19] GPC Canada. Albertan's awareness of and views on privacy issues, 2000.

[20] Harris-Equifax. Health information privacy survey, 1993.

[21] Harris Interactive. Health-care professionals, pharmacies, hospitals gain the public's top trust. *Health Care Poll 3*, 2 (2004).

[22] Harris Interactive. Many nationwide believe in the potential benefits of electronic medical records and are interested in online communications with physicians. *Harris Health Care Poll 4*, 4 (2005).

[23] Harris Interactive. Press release: Health information privacy (hipaa) notices have improved publics confidence that their medical information is being handled properly, February 24 2005.

[24] Hoffman, D. L., Novak, T. P., and Peralta, M. Building consumer trust online. *Communications of the ACM 42*, 4 (1999), 80–85.

[25] Jones, S., Wilikens, M., Morris, P., and Masera, M. Trust requirements in e-business. *Communications of the ACM 43*, 12 (2000), 81–87.

[26] Koufaris, M., and Hampton-Sosa, W. The development of initial trust in an online company by new customers. *Information and Management 41*, 3 (2004), 377–397.

[27] Mandl, K. D., Szolovits, P., Kohane, I. S., Markwell, D., and MacDonald, R. Public standards and patients' control: how to keep electronic medical records accessible but private commentary: Open approaches to electronic patient records commentary: A patient's viewpoint. *BMJ 322*, 7281 (2001), 283–287.

[28] Menduno, M. apothecary.now. *Hospitals and Health Networks July* (1999), 25–36.

[29] POLLARA. Nurses, doctors still top the pollara public trust index, 1998.

[30] POLLARA. Public trust index 2000, 2000.

[31] POLLARA. Health care in Canada survey retrospective 1998-2003, 2003.

[32] Princeton Survey Research Associates. Medical privacy and confidentiality survey, 1999.

[33] Radwanski, G. Condition critical: Health privacy in Canada today, 2001.

[34] Roy Morgan Research. Community attitudes to privacy, July 2001.

[35] Salam, A., Iyer, L., Palvia, P., and Singh, R. Trust in e-commerce. *Communications of the ACM 48*, 2 (2005), 72–77.

[36] Saskatchewan Health - Policy and Planning Division. Consultation paper on protection of personal health information, April 1998.

[37] The White House. Transforming health care: The presidents health information technology plan, 2004.

[38] Willison, D. J., Keshavjee, K., Nair, K., Goldsmith, C., and Holbrook, A. M. Patients' consent preferences for research uses of information in electronic medical records: interview and survey data. *BMJ 326*, 7385 (2003), 373–390.

[39] Woolhandler, S., Campbell, T., and Himmelstein, D. Costs of health care administration in the United States and Canada. *New England Journal of Medicine 349*, 8 (2003), 768–75.