Electronic Personal Health Record Systems: A Brief Review of Privacy, Security, and Architectural Issues

David Daglish and Norm Archer
daglised@mcmaster.ca archer@mcmaster.ca
DeGroote School of Business, McMaster University

Abstract

Electronic personal health records (PHRs) are beginning to receive widespread attention as a tool for consumers. Such systems may be used by individuals to input data and to access information from a variety of sources (e.g. family physicians), thus improving their understanding of the state of their health and helping to manage their own healthcare better. The main source of information for PHRs is normally the patient's physician, supplemented by patient input and other sources of information such as prescriptions and lab test results, as well as institutional inputs from hospitals and other facilities. The architecture of such a system must be such that patients can access all the useful information that is relevant to their medical history in a form that is understandable to them, while at the same time protecting against unauthorized access. This paper addresses design and architectural issues of PHR systems, and focuses on privacy and security issues which must be addressed carefully if PHRs are to become generally acceptable to consumers.

1. Introduction

Computers have been in use in hospital health care in Canada for many years, beginning with administrative record keeping and clerical functions, and evolving more recently to creating and maintaining clinical patient records and other medical data. A recent survey of Canadian hospitals [1] indicated that only about half were using electronic clinical records. In most cases, hospital computerization has not led to interoperable systems, leading to situations where systems used in hospitals and areas within them are silos of information, with little interconnection or transfer of electronic information to other institutions as recommended by modern business best practice. Much of this can be blamed on the lack of adoption of electronic health record and system standards.

Meanwhile, Canadian doctors continue, for the most part, to maintain paper-only clinical records in their practices, with only approximately 25 percent using electronic medical record systems [2]; most of the computer systems in use in medical practices support only administration and billing.

Recent advances in information technology (IT) have introduced new systems that can support healthcare delivery, patient support, and education. This in turn enables a redesign of health care processes that are supported through the integration of electronic communication and healthcare records. Healthcare IT can empower patients and give them a role beyond the past environment of being a passive recipient of healthcare services, to an active role in which the patient is informed, has choices, and is involved in the decision-making process. Such a role, called patient-centred healthcare, is becoming popular in Western healthcare systems, since it can engage patients in managing their own healthcare, with better outcomes at lower costs. For patients to be effective in such a role requires access to much more information about their healthcare history and about healthcare topics that relate specifically to their diseases or condition. This is why Personal Health Records (PHRs) – what they are, what they should include, how they can be provided, and how they can be accessed without compromising security and privacy – are becoming much debated topics.

In addition, the generally wide availability of health-related information on the Internet has led healthcare consumers to become more active in searching online for general medical information to educate themselves on best medications, treatments, and lifestyle choices for themselves and their families. In Ontario, the *Ministry of Health and Long Term Care* (MOHLTC) has also increased its efforts to move some forms of healthcare into the community and away from institutions—the *'Aging at Home'* initiative, for example [3]—which would necessitate the flow of health information from healthcare institutions and practitioner offices to patients and community care providers, and in the

978-0-7695-3805-1/09 $26.00 © 2009 IEEE
DOI 10.1109/CONGRESS.2009.14

reverse direction from patients to institutions and practitioners. This need is mirrored in the plan to have a cross-Canada exchangeable format for electronic health records by 2010 [4] and the recent announcement of the goal for every resident of Ontario to have an electronic personal health record by 2015 [5]. These initiatives are absolutely critical to progress in the widespread development and introduction of PHRs because the supporting system architectures, as we will show, depend to varying degrees upon agreed electronic health record standards for gathering and communicating patient record information.

PHRs are considered to be patient centred health and/or medical records in electronic form that are accessible to patients themselves, but there is no consensus on what information they should include. The term PHR as used in this paper will refer both to the records themselves and to the information systems used to support them so they can be created, updated, corrected, and accessed by patients/consumers and by their healthcare providers. Also in this paper, the term 'patient' will be used interchangeably with 'consumer'. At any given time, most consumers are not patients, but all consumers will be patients at some time. It is as consumers of healthcare resources that individuals make decisions to manage their own health with the support of others (general practitioners, specialists, nurses, family, and other providers) in their circle of care.

The use of PHRs to help get patients involved in managing their own care and thus improve their health outcomes is well-motivated. In a published literature review [6] of 109 articles covering 112 PHR system descriptions (with 31 appearing in more than one report) it was determined that the majority of the articles reported positive results in improving the level of care; about two-thirds of the peer-reviewed articles reported positive findings, as did 94 percent of the uncontrolled experiments. The articles covered primarily chronic illnesses, such as diabetes, heart diseases, mental health issues, and multiple disease cases. In the instances where there was a randomized controlled trial, there was overall a positive correlation between exchanging data using a PHR and positive health outcomes ($r=0.28$, $p=0.05$).

The purpose of this paper is to discuss certain issues concerning the general implementation of electronic personal health records, based on a review of the literature. This review included the healthcare literature (Medline), the information systems literature, the information technology literature, and the Web, using keyword phrases such as personal health records, electronic health records, and electronic medical records. In this paper, Section 2 discusses security and privacy issues that affect the design and operation of PHRs, Section 3 presents a discussion of possible PHR architectures that have been proposed, pilot tested, or implemented, Section 4 compares some of the attributes of different PHR architectures, and Section 5 is a concluding discussion of the findings of this study.

2. Security and Privacy

Consumer perceptions of privacy and security of health records are critical to the maintenance of trust with their healthcare providers and ultimately their acceptance of electronic health records, whether or not they are for personal use. However, providing PHRs to consumers opens more potential avenues for security and privacy violations because of the large size of the population that would have controlled access to these records. In a recent U.S. survey [7], four percent of American adults believed that they or a family member had confidential personal medical information either lost or stolen.

A recent Canadian survey addressed perceptions related to electronic health records [8]. Findings included: a) trust in health professionals was very high, b) 87% indicated that timely and easy access to personal health information is integral to the provision of quality health care, c) about half of the respondents were concerned about serious mistakes in diagnoses or treatment due to incomplete, inaccurate, or illegible information, d) four percent of the respondents reported that their health information had been used inappropriately or without their consent, e) 77 percent would like audit trails in place that would document access to their health information, f) 74 percent want strong penalties for unauthorized access, and g) 66 percent want clear privacy policies to protect health information.

In an age of identity theft and data snooping, it is not surprising that there is a concern for security and privacy in PHRs. Systems can be encrypted and password protected, but that is not necessarily sufficient in the case of bad systems or poorly chosen passwords [9]. If security and access methods are too strict or cumbersome, many of the benefits of accessibility and timeliness are eroded. Improper disclosure of information is a problem for patients, depending on to whom the disclosure is made. For example, there are concerns about what insurance companies may do if certain information is improperly disclosed to them. With professional medical practitioner support being critical to the success of PHRs, the concept of invasion of privilege is also one not to be dismissed [10]. Doctors have long had sole responsibility for managing their

records, and may not be trusting of the data provided by others through a PHR.

Conventionally, a PHR system involves networked computers working together to perform the overall system tasks for the purpose of separation of work load, separation of function, or separation of data. Multiple systems sharing a load provide enough processing capacity to respond to and service the requests for information from multiple actors within the network [11]. Separation of data prevents data from being compromised through physical theft or indirect access; this could be through separation of health data from the identifying data stored in the form of registries [12]. For example, Enterprise Master Patient Registries (EMPIs) [13] have been developed in a number of Canadian jurisdictions to provide centralized support to identify records belonging to particular patients that are distributed among several systems but do not have common unique identifiers.

Another technique is to separate the encrypted data from the keys necessary to decrypt it [14]. In the separation of functions approach, different functional tasks are performed on separate systems, either physical or logical, for the purpose of isolating replaceable or exchangeable functions. In the open source *Indivo* software[1] that has been used as the basis for some PHR systems, for example, the functional breakdown is into user interface, data storage, and business logic [14]. This architecture allows the user interfaces to be flexible, customizable and adaptable if necessary to the specific user population, and the data storage optimized for best security and privacy protection, with no impact on business logic. Business logic includes access policies and their enforcement, based on data records that are gathered and consolidated into a coherent personal health record [14].

In some cases, descriptions of the architecture of a system that controls sensitive data such as health records can be used to alleviate concerns in the public view, based on their perceptions of risks and security methods. One of the key concerns is unauthorized access, which can be prevented by proper authentication. Authentication is traditionally a username or identity (ID) with an associated password, but these have been superseded by other, more robust methods [15]. More secure authentication is generally based on two or more of: something the user knows, something defining where the user physically is, something relating to who the user is, or something that the user physically possesses [15]. If one focuses on the physical location as one of the parts of authentication, then that would limit the access to the patient's record to a set number of places, where trusted provider personnel are located (e.g. hospitals, clinics, or doctors' offices). In that regard, generating user access and establishing credentials from a trusted source has been proposed to be a critical issue for proper authentication. Building on the inherent trust in a doctor-patient relationship by having the physical locations of the primary points of contact in a doctor's office, clinic, or hospital provides a solution to the system trust issue [14]. Alternative access includes providing the security information necessary through the regular mail, through current validated World Wide Web techniques such as a valid security certificate from a trusted organization, or through some other trusted third party [14].

2.1 Implementing PHR Security

In order to provide the necessary level of security for PHRs, several mechanisms have been proposed. The primary issue is that any security mechanism needs to be usable, or the users will not use it [16], either circumventing security, choosing another system to use, or not using a system at all. There is no way to ascertain where a malicious intruder may attempt to access, intercept, or physically remove data, so encryption and denying access to the data without permission needs to be active at all stages of the system [16]. However, not all encryption is good encryption [9] and some commercial products do not provide the protection expected by the consumer. This is not something that a user would be able to determine without technical assistance, potentially leaving data exposed to a knowledgeable data thief.

Wright and Sittig [9] further recommend that data protection be incorporated into any future standards developed for PHRs. *Public Key Infrastructure* is both an authentication and encryption technology that could be used to satisfy both issues, but it requires significant memory and processing capacity. It has been suggested [15] for example, for wireless systems that technological advances in portable devices such as newer cellular telephones that can run small applications could be a solution to the key retention issue. However, this solution is not easily scalable to large user populations, and it requires specialized equipment to interface with wireless devices. Finally, patients need to be in control of their data and the authorization of various providers to access and/or to add information [17], so that those responsible for the patient's care can perform efficiently.

[1] http://www.indivohealth.org/

Some systems that have been developed have broken data access into classes, defined roles for the users that guide the access in the system, and enabled the patients and administration to assign rules for which class of data is available for which class of user, or to specific users [17, 16]. Levels of information that have been used are: non-identifying, general health, sensitive, parent-sensitive, and patient-sensitive. In this approach, the restrictions or sensitivity increase as one moves along the list. Parent-sensitive data can be discussed with patients who are not yet adults, but defined in law to be able to manage some of their own affairs; pregnancy and abortion information for teens over 16 is in this category in many jurisdictions. Patient sensitive data is information that should not be available to the patient for the patient's own well-being in the view of the physician entering the data [16]; this may be a permanent state, or transitory—allowing for a face-to-face discussion of sensitive information rather than impersonal discovery in the PHR.

Stakeholder roles in PHR systems include: researcher, patient, primary care, secondary care, emergency care, and administration. In the foregoing schemes, a researcher can access data in broad groups, but no identifying information is available that can identify specific patients, but an emergency room physician can easily find the current list of medications and prior history of a patient in order to deliver the appropriate health care with reduced risk [12]. Further refinement would include patient-defined or administration-defined rules, so that a patient may define who may see and/or add to the record, but the administrator can prevent a patient from inadvertently creating a leak while at the same time permitting reasonable operations [14]. These rules have been implemented at the business logic level in *Indivo* [14] or at the database access level [17].

Once the security system has been established, an audit function is needed so users or administrators can review the list of accesses to the PHR data, and any unauthorized breach can be detected and acted upon [4]. Health care providers need to accumulate data about patients to be able to treat them effectively and be paid for their services, so there is a need for them to be able to access the data, but at the same time it is necessary to guard the data against unwanted breaches. There are several pieces of legislation in Canada that govern expectations for the practitioners and provide penalties for failing to exercise care in managing the data [4]. Since Canadian provinces are responsible for healthcare, each province has enacted its own health information privacy acts. For example, Ontario has its *Personal Health Information Protection Act* (PHIPA).

PHIPA is designed to allow providers to collect and use personal information in the process of providing health care to patients. The definition of a provider of health care—called a health information custodian in the Act—includes most of the traditional groups who provide health care, as well as the institutions that they usually work at or for. Thus doctors, nurses, dentists, hospitals, boards of health, community health workers and agencies, long-term care facilities, ambulance and emergency services, and the *Ontario Ministry of Health and Long Term Care* (MOHLTC) itself. Consent for 'normal' use of PHRs is generally implied by the individual who provided the data in the first case, but if the data are to be disclosed to someone who is not, or does not work for, a health information custodian, consent must be explicitly given. An individual may specifically deny access or disclosure to certain health information custodians or health care providers in advance, and it is required for the custodian that is being asked for information to disclose the denial of consent to the requesting person or organization. Systems that are created to allow the custodians to gather, use, update, or distribute the data must also comply with the requirements of the act and to protect from unnecessary disclosure, or other misuse or unauthorized access.

An important final note on privacy concerns is that the patient/customer is the ostensible owner of their data that reside within, or can be accessed by, a PHR system. In such a system the data owner has the right to permit or deny access to any or all of the data to any or all individuals, including caregivers. If the PHR system is properly configured, the owner manages his or her own privacy, thus arguably eliminating many of the concerns about privacy controls that threaten most online health records systems.

3. PHR System Architectures

Discussions of PHR content invariably refer to the origin of accessible information that may be used in the PHR, and therefore a driver of the system architecture. Potential architectures can be thought of as a continuum that ranges from tethered to standalone, with the complexity of the architecture rising from low values, representing simplicity, at the ends of this continuum to peak complexity in the middle.

3.1 Tethered PHRs

At one end of the continuum, a 'tethered' PHR is a system that is connected in some way to one organization's system (typically the family doctor's system, referred to as an EMR or Electronic Medical Record system, or an institutional system, referred to as an EHR or Electronic Health Record system) and accessible by the patient. Tethered PHRs offer the advantage of healthcare practitioner input, but this is normally limited to those associated with or practicing within the organization that hosts the PHR. Since there is a base organization, there is likely to be a form of backup, either by reloading the personal copy of the information from the source, or through corporate backups. Unfortunately, when the patient changes affiliation from the host institution to an alternate source, the data may not be transferrable due to record and/or system incompatibilities.

3.2 Standalone PHRs

At the other end of the continuum, a 'standalone' PHR may take on one of two possible forms:

a) Smartcard PHRs are where patient data is stored on some portable media such as a smartcard, supported by software that can be accessed by computer to view, enter, modify, or organize the data. This type of PHR is (at least in concept) simple and convenient, and may be portable (e.g. a 'smart' healthcard such as the system now planned for 85 million German citizens [18]). However, there is little protection from loss, theft, or damage [10], unless there is online network backup. In past tests run on devices with commercial PHR software in this category, there was either no encryption to protect the personal data, or there was poor encryption that was easily defeated, and it was based on flawed software with known weaknesses [9]. Standalone PHRs may also be primarily patient driven, in which case they are less likely to be used or trusted as a method of communicating medical data among healthcare practitioners. Further, unless the patient has a strong motivation to keep the information current, much valid data will not be entered, or will be out of date [10]. However, if they are state developed and sanctioned, with proper security and privacy controls, as in the German smartcard system currently being implemented [18] they may be regarded as trusted PHRs by both institutions and practitioners. Recently, it appears that the German system has experienced opposition from physicians who have voiced concerns about privacy violations [19].

b) Consolidator PHRs are in the form of centralized Internet portals in which the patient can enter his/her own data and which also gathers data from other sources such as primary care facilities, healthcare institutions, etc. where the patient has been served and where electronic records of the engagements have been maintained. Commercial portals that support patient-driven consolidation [20] are the basis of advanced web-based PHR systems such as *Microsoft's HealthVault* and *Google's Google Health*, where patients can gather their own health data and enter it into the system. These systems may also link to other sources of information such as clinics or healthcare institutions in order to gather additional provider supplied patient records. In some cases there are tools to aid in the importation from well-known systems or to aid in identifying the correct or relevant information in the health file [21].

3.3 Integrated PHRs

The 'integrated' PHR is system driven, and gathers and presents patient data from multiple sources into a single view. Integrated systems are complex, but the complexity yields usability and flexibility [10]; they also imply a central regional site that gathers the accumulated data with associated access protection and presentation tools. When the connection between the central site and the data source or data user is considered, there can be several options and issues. One such option is a central system that collects health information for all patients based on information that patients and their providers have selected to be stored and available [20]. This is referred to as a 'push' model, based on the concept of pushing the data from the gathering point to the central site.

A second option is to ensure interoperability and comparable utility of the data generated at all points in the health care system so that they can all be gathered at central points [20]. This is referred to as a 'pull' model, since the central agency requests all the data needed from the providers. Note that the pull model does not necessarily involve a central repository, since data may only be requested when needed by a requesting user/patient. This architecture has the advantage that there is no duplication in a central store of the information being accessed, and that it accesses the latest information about the patient as needed. It has the disadvantage that such searches may take a long time to complete and it places additional overhead burdens on the communication network and the source systems being accessed, to eliminate points of failure or loss.

Integrated systems offer a blend of simple PHR and normal EMR/EHR data, providing input from multiple sources—patients and practitioners—with secure backup of the data. An example of such a system is the U.S. Department of Veteran's Affairs' MyHealtheVet portal that allows over half a million veterans to access their personal health records online [22]. Integrated systems are generally implemented as portals with either secure Internet access [12] or dedicated kiosks [23]. Additional functionalities may be offered, such as terminology translation or definitions, video attachments for remote diagnosis, or biometric—e.g., blood pressure, or blood sugar monitoring and tracking.

3.4 Other PHR Models

Other approaches have been proposed to deal with the diverse nature of health data and distributed sources of data, including a subscription model. In this model [14], a patient establishes a PHR on the system and identifies sources of personal health data. The system administrators then define an agent to query the source periodically, looking for new data for all clients who have identified that facility as a data source. The agent will then transform the data from the original source into a form that is more appropriate for the system and store it in the database. The source of the information must also be maintained so that changes in the original source may be captured.

In addition to the patient, healthcare providers are the primary source of PHR medical data. Doctors, nurses, consultants, and other medical personnel generate the medical data in the course of caring for the patient and performing their normal duties, either in general practitioner offices or clinics, walk-in clinics, or healthcare institutions. These data sources normally provide such feedback directly to the patient's family doctor. Full videos and analysis of tests such as ultrasounds or x-rays, or behavioural observations can also be transmitted or stored directly in the patient's records. Medication renewals and alerts can provide feedback on compliance to the prescribing physicians. In combination with data entered by the patient, when data available to the patient's physician or other care providers are also made accessible through the patient's PHR, this can give the patient a full view of his or her medical history. Several PHR implementations [12] have an emergency data section that is available to emergency personnel involved in the provision of health care, providing data such as medication sensitivities and other medical information during emergency interventions.

4. Comparison of Proposed PHR Architectures

Each of the PHR architectures, from standalone to tethered, has some benefits to convey to the users and promote its use, but each carries some limitations or liabilities that may discourage usage. Although this paper is far too brief to describe all such limitations, we have listed in Table 1 some of the more important attributes of each architecture that are relevant to the foregoing discussion. Complexity, access, and data sources define the architecture in terms of some operational characteristics. Major risks, security, and privacy help to define the limitations and possible barriers to acceptance. And finally, example installations and comments provide real world qualifications. This allows a direct comparison among the architectures, and gives a general, albeit simplified view of how and where future PHR systems may evolve.

Tethered architectures are conceptually simple since they extend existing EMR systems, with separate applications for consumer data entry, management, and display, and controlled secure access to their clinic's EMR clinical records. Because access is controlled by the clinic, decisions on which clinical information consumers will be able to access may vary significantly, depending on the consumer's physician. This type of system is under trial at several Canadian clinics. They will not be feasible at clinics or medical offices with one or a small number of practitioners and limited support staff, unless their EMR operations are outsourced to larger organizations which have the technical and administrative staff to support PHRs. No standard EMR record and application specifications have been implemented in Canadian provinces, but shortlists of acceptable commercial EMRs are maintained in each province, and there is a central agency that collects ratings from EMR users [24]. Thus consumers moving to different clinics and/or provinces will probably experience major problems when they attempt to move their PHRs to their new environments.

Table 1. Summary of Some PHR System Architecture Attributes

Attribute	PHR System Architecture		
	Tethered	Integrated	Standalone
Complexity	Relatively simple (conceptually)	High. Need to establish and maintain data source standards	*Smartcard:* Simple, but backup complex *Web-based Consolidator:* Moderate. Network links to consumers, practitioners, etc.
Access	Portal or client server	Internet portal	*Smartcard:* Card or memory stick readers *Consolidator:* Internet portal
Data Sources	Primary care server, pulling data from other sources (test labs, etc.)	Pull Model: Central source, pulling from multiple primary sources Push Model: Central source, receiving data pushed from multiple primary sources	*Smartcard:* Direct from all sources *Consolidator:* Network connections to consumers, practitioners, institutions.
Major Risks	Access control by primary care physician or institution might be too restrictive. Data entry by consumer may not be allowed. Transfer to other systems may be problematical	Acceptance and maintenance of common standards among data sources. Integration of networks and systems requires high-level collaboration	*Smartcard:* Loss or theft of device; Each provider requires standards to link to and use smartcard. *Consolidator:* Non-standard data sources and consumer IDs that must be accommodated; Privacy controls may be lax
Security	Secure extranet portal. Requires additional support beyond normal primary care server	Managed centrally with suitable levels of encryption and access control	*Smartcard:* Limited by power of onboard CPU *Consolidator:* Acceptable if encryption used
Privacy	Managed by consumer's primary care site	Access managed through central system, based on consumer access level request controls	*Smartcard:* Physical access controlled by consumer *Consolidator:* Data controlled by consumer
Example Installations or Trials	MyOscar [25]	U.S. DVA [22]	*Smartcard:* Germany [18] *Consolidator:* HealthVault [26]
Comments	Appropriate only for multiple physician clinics with staff support available	Multiple copies of data result if stored in central repository. If not stored, access delays likely to be unacceptable	*Smartcard:* May be costly to evolve system and standards *Consolidator:* Requires access permission and ability to adapt to multiple data sources

The integrated architecture is the most complex considered, but it appears to be the architecture of choice in the Canadian healthcare system. Various pieces of this architecture are gradually taking form, depending on the province. Of critical importance is the development and acceptance of a common record standard, at least within each provincial jurisdiction, since it will be difficult to manage fully integrated systems without well defined standards. This is of concern, given the fact that most healthcare institutions don't have agreed standards as yet, and those primary care clinics that have adopted commercial EMRs are a long way from adopting standard record designs. One possible solution that was recently announced in Ontario, for example, is a disease specific centralized approach (e.g. diabetes) that will maintain a central provincial record system for patients that presumably will be receiving data pushed from multiple physicians and clinics across the province. In this way, if physicians are required to provide data, it will be in their best interests to adopt some sort of standard record. Although

patients will have access to this system, it is not clear whether they be able to enter data.

The Web-based Standalone Smartcard architecture has received little attention in North America but is currently being proposed for rollout in Germany. This is expected to generate a significant amount of data as its implementation continues. Although smartcards are conceptually simple and highly portable, and similar to 'chip and PIN' bankcards now being adopted widely in Canada, these smartcards will contain a large amount of sensitive information and will be susceptible to theft and loss. Security will be more difficult to maintain at a high level, and network backup facilities will need to be provided in case of theft or loss. The German project has recently encountered significant delays due to opposition from physicians concerning privacy and security issues.

The Standalone Consolidator architecture has been developed by several major U.S. commercial firms who currently have several U.S. sites under trial, one at a major clinic [26] and another at one of the largest U.S. Health Maintenance Organizations (HMOs). These systems accept consumer inputs but they also depend on standardized health records that are in place at the source organizations, where security, privacy, and access privileges will obviously be a major concern. This is even more of concern, given the rumours that some such systems plan to fund their operations through the sale of patient data to commercial organizations that may not have the best interests of consumers in mind. In a sense when these systems are operated in such an environment they are similar to tethered systems but with their own separate databases. How successful consolidators will be when records must be gathered from a variety of sources is still open to question.

5. Discussion

In general, patients want to be able to access and control their own health records through online access [27, 28]. There are several reasons why patient access can be important. First, records may be missing or incomplete as a result of a patient having being seen by several doctors at varied locations that are not part of the same larger support system, so having patient accessibility can be employed positively to validate, verify, and fill in the records for the primary care team [29]. Second, for chronically ill patients, many studies have shown that a PHR can be a contributing factor in positive outcomes, with a notable correlation between active PHR use and health outcomes [6]. Reasons given for this effect are varied, but the use of the PHR by the care team as a communication and activity tracking method, and active participation in self management of patient health care in order to achieve and maintain good health [30] have been cited. Further, for patients in emergency department settings, the existence of PHRs would be extremely helpful and would be almost certain to save lives by improving the speed and accuracy of staff response. Third, under the privacy act, individuals may access their own health records, except where it is professionally judged to be harmful, or if such disclosure is legally prohibited.

Fourth, unfortunately not all patients take their healthcare seriously enough to take the steps suggested even when presented with a PHR showing negative results [29]. Finally, while parents generally participate in providing a healthy start for their children, their interest in continuing the support of a PHR for their children does decline over time [31]. Although there have not as yet been studies to verify this conjecture, it seems likely that unless there is a direct and identifiable risk to health, patients or caregivers will not be motivated to take the maintenance and use of a PHR seriously. Those who are more likely to do so include the parents of disabled children, people with serious chronic illnesses, people such as athletes with a strong interest in wellness, and caregivers for the elderly at home.

We have noted that the content of a PHR can be important to maintaining a patient's health, and it can also be useful to the healthcare provider. The professionalism of the content's presentation is not as important as content that provides value to the patient, particularly if it can be customized to the patient's specific case through analysis of the content and its presentation, or links to other helpful and supporting information. Many patients are concerned over privacy and security issues surrounding PHR data Also of concern to patients is that, given access to medical notes in the PHR, they will have to become more conversant with medical terminology and related details in order to understand and take corrective action to maintain or improve their health [30].

In conclusion, the general indications are that there are significant benefits to PHR use, although there are architecturally specific risks to their adoption (see Table 1) that must be considered. Some of these relate directly to consumer concerns about security and privacy, and we have attempted to discuss these in the context of several different PHR system architectures that have been proposed or are in trial. In Germany, the choice of the standalone smartcard PHR is close to national implementation. In the United States, implementations and/or tests of all the suggested architectures except the standalone smartcard are underway. In the United Kingdom, the National Health Service (NHS) appears to have

settled on an integrated architecture for PHRs [32]. It is also becoming clear that Canadian healthcare agencies are settling on integrated architectures for electronic patient health records [4]. PHRs will of necessity tap into these systems eventually, so this architecture is probably representative of future PHR architectures in Canada. This also fulfills the desire for a durable, longitudinal collection of health data as captured in the many definitions of what a PHR is supposed to be. We have seen that an integrated PHR is able to take its content from many sources, which reflects the reality of the patient experience, with many providers and institutions involved in providing care over time. The standards efforts are moving ahead [33] but better forms of data collection and storage have evolved in the past, and this trend is not likely to stop; an integrated PHR, with its many systems and layers within its architecture, is best situated to move along with the technological evolution. In a similar vein, with a distributed system, the presentation is capable of being customized for different users, or changed over time to suit the medical education and evolution of the active consumer [14].

In order for most of the possible architectures to be useful, the content needs to conform to an accepted and interoperable standard, or set of standards; this work is advancing internationally [33, 34] but without clear definitions, the data may not be shared reliably, rendering some sources incompatible with the patient's PHR. Funding the development of standards and providing the necessary infrastructure is another issue that stands to delay or otherwise impede the efforts to bring PHRs to Canadian consumers; some money has been pledged, but more will be necessary [35]. A matter of great importance is that family physicians who actively use EMRs (Electronic Medical Record systems) for the clinical records of their patients will play an essential and central role in any implementation of PHRs. However, the low current rate of EMR adoption by family physicians, except in multiple partner practices, will continue to be a significant barrier to general adoption of PHRs in Canada for some time.

6. References

[1] S. Urowitz, D. Wiljer, E. Apatu, G. Eysenbach, C. DeLenardo, T. Harth, H. Pai, and K. Leonard, "Is Canada ready for patient accessible electronic health records? A national scan," *BMC Medical Informatics and Decision Making*, vol. 8, pp. 33, 2008.

[2] S. Chernos, "Cross-country check-up http://www.canhealth.com/doctors.html#D07octstory1 (accessed March 9 2009)," in *Technology for Doctors*, 2007.

[3] MOHLTC, "Aging At Home Strategy Backgrounder: Ministry of Health and Long Term Care." Toronto: Queen's Publisher, 2007.

[4] CHI, "White Paper on Information Governance of the Interoperable Electronic Health Record (EHR) http://www2.infoway-inforoute.ca/Documents/Information%20Governance%20Paper%20Final_20070328_EN.pdf (Jan 8 2009)," Canada Health Infoway, Montreal 2007a.

[5] MOHLTC, "Ontario integrates e-health activities under one agency: Ministry of Health and Long Term Care http://www.health.gov.on.ca/english/media/news_releases/archives/nr_08/sep/e_health_nr_20080929.pdf (Jan 9 2009)." Toronto: MOHLTC, 2008.

[6] D. Dorr, L. M. Bonner, A. N. Cohen, R. S. Shoai, R. Perrin, E. Chaney, and A. S. Young, "Informatics Systems to Promote Improved Care for Chronic Illness: A Literature Review," *Journal of the American Medical Informatics Association*, vol. 14, pp. 156-163, 2007.

[7] HarrisInteractive, "Millions believe personal medical information has been lost or stolen http://www.harrisinteractive.com/harris_poll/index.asp?PID=930 (Jan. 7 09)," HarrisInteractive, 2008.

[8] CHI, "Electronic health information and privacy survey: What Canadians think - 2007 http://www2.infoway-inforoute.ca/Documents/EKOS_Final%20report_Executive%20Summary_EN.pdf (Jan 7 2009)," Canada Health Infoway 2007b.

[9] A. Wright and D. F. Sittig, "Encryption Characteristics of Two USB-based Personal Health Record Devices," *Journal of the American Medical Informatics Association*, vol. 14, pp. 397-399, 2007.

[10] P. C. Tang, J. S. Ash, D. W. Bates, J. M. Overhage, and D. Z. Sands, "Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption," *Journal of the American Medical Informatics Association*, vol. 13, pp. 121-126, 2006.

[11] W. W. Simons, K. D. Mandl, and I. Kohane, "The PING Personally Controlled Electronic Medical Record System: Technical Architecture," *Journal of the American Medical Informatics Association*, vol. 12, pp. 47-54, 2005.

[12] F. Ueckert, M. Goerz, M. Ataian, S. Tessmann, and H.-U. Prokosch, "Empowerment of patients and communication with health care professionals through an electronic health record," *International Journal of Medical Informatics*, vol. 70, pp. 99-108, 2003.

[13] C. Sobun, "EMPI allows networks to integrate medical records," *IT Health Care Strategist*, vol. 2, pp. 10-13, 2000.

[14] K. D. Mandl, W. W. Simons, W. C. R. Crawford, and J. M. Abbett, "Indivo: a personally controlled health record for health information exchange and communication," *BMC Medical Informatics and Decision Making*, vol. v7, pp. 1-10, 2007.

[15] U. Sax, I. Kohane, and K. D. Mandl, "Wireless Technology Infrastructures for Authentication of Patients: PKI that Rings," *Journal of the American Medical Informatics Association*, vol. 12, pp. 263-268, 2005.

[16] D. B. Baker and D. R. Masys, "PCASSO: a design for secure communication of personal health information via the internet," *International Journal of Medical Informatics*, vol. 54, pp. 97-104, 1999.

[17] R. Agrawal and C. Johnson, "Securing electronic health records without impeding the flow of information," *International Journal of Medical Informatics*, vol. 76, pp. 471-479, 2007.

[18] Gesundheitskarte, "German electronic healthcard http://www.healthcareitnews.eu/index.php?Itemid=&option=com_search&searchword=gesundheitskarte (Jan 7 2009)," Europe Healthcare IT News, 2008.

[19] N. Ernstmann, O. Ommen, M. Neumann, A. Hammer, R. Voltz, and H. Pfaff, "Primary care physician's attitude towards the German e-health card project - Determinants and implications," *Journal of Medical Systems*, 2008.

[20] D. T. Gunter and P. N. Terry, "The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions," *J Med Internet Res*, vol. 7, pp. e3, 2005.

[21] I. M. Kim and B. K. Johnson, "Patient Entry of Information: Evaluation of User Interfaces," *J Med Internet Res*, vol. 6, pp. e13, 2004.

[22] InterSystems, "The U.S. Department of Veterans Affairs uses InterSystems Ensemble to integrate 130 systems and improve patient care http://www.intersystems.com/casestudies/ensemble/usdva.pdf (Jan 6 09)," InterSystems Ensemble Case Study, 2008.

[23] R. Jones, "Making health information accessible to patients," *Aslib Proceedings*, vol. 55, pp. 334-338, 2003.

[24] Canadian EMR, "Online source of information on products and services in Canada for the EMR-based practice http://www.canadianemr.ca/index.aspx?PID=2 (Viewed March 8 2009)." Vancouver, British Columbia: Canadian EMR, 2009.

[25] D. Chan, "Welcome to MyOSCAR - Your Personally Controlled Health Connection http://www.stonechurchclinic.ca/myoscar (Jan 7 2009)." Hamilton, Ontario: Stonechurch Family Health Centre, 2008.

[26] Anonymous, "Microsoft Healthvault scores big win: Pilot with Kaiser http://www.networkworld.com/community/node/28560 (Jan 7 2009)," in *Network World*, 2008.

[27] G. K. Adler, "Web Portals in Primary Care: An Evaluation of Patient Readiness and Willingness to Pay for Online Services," *J Med Internet Res*, vol. 8, pp. e26, 2006.

[28] I. C. Denton, "Will Patients Use Electronic Personal Health Records? Responses from a Real-Life Experience," *Journal of Healthcare Information Management*, vol. 15, pp. 251-9, 2001.

[29] M. Staroselsky, L. A. Volk, R. Tsurikova, L. Pizziferri, M. Lippincott, J. Wald, and D. W. Bates, "Improving electronic health record (EHR) accuracy and increasing compliance with health maintenance clinical guidelines through patient access and input," *International Journal of Medical Informatics*, vol. 75, pp. 693-700, 2006.

[30] M. A. Earnest, S. E. Ross, L. Wittevrongel, L. A. Moore, and C.-T. Lin, "Use of a Patient-Accessible Electronic Medical Record in a Practice for Congestive Heart Failure: Patient and Physician Experiences," *Journal of the American Medical Informatics Association*, vol. 11, pp. 410-7, 2004.

[31] A. J. Hampshire, M. E. Blair, N. S. Crown, A. J. Avery, and E. I. Williams, "Variation in how mothers, health visitors and general practitioners use the personal child health record," *Child: Care, Health and Development*, vol. 30, pp. 307-316, 2004.

[32] NHS, "NHS Care Records Service http://www.nhscarerecords.nhs.uk/ (accessed March 9 2009)." London, UK: National Health Service, 2008.

[33] CHI, "Standards Collaborative: Enabling solutions, enhancing health outcomes together http://www.infoway-inforoute.ca/Admin/Upload/Dev/Document/R2_ENGLISH%20SC%20Guide%20and%20Standards%20Catalogue.pdf," Canada Health Infoway, Ottawa, Ontario 2008.

[34] G. D. Katehakis, S. Sfakianakis, M. Tsiknakis, and C. S. Orphanoudakis, "An Infrastructure for Integrated Electronic Health Record Services: The Role of XML (Extensible Markup Language)," *J Med Internet Res*, vol. 3, pp. e7, 2001.

[35] CHI, "The Infoway approach http://www.infoway-inforoute.ca/lang-en/about-infoway/approach (accessed March 9 2009)." Toronto, Ontario: Canada Health Infoway, 2009.