MeRC

McMaster eBusiness Research Centre

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

by

David Daglish and Norm Archer

McMaster eBusiness Research Centre (MeRC)

WORKING PAPER No. 27
January 2009

McMaster University

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

by

David Daglish and Norm Archer
McMaster University

daglised@mcmaster.ca
archer@mcmaster.ca

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 their own personal 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 how 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.

Keywords: Personal health records, architecture, privacy, security

INTRODUCTION

Computers have been in use in hospital health care in Canada and other countries 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. Only about half of Canadian hospitals use electronic clinical record systems (Urowitz, Wiljer et al. 2008). Hospital computerization has usually not led to interoperable systems, resulting in 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. Much of this can be blamed on the lack of adoption of electronic health record and system standards. Canadian doctors have also been slow to adopt electronic clinical records, with only about 25 percent currently using such systems (Chernos 2007).

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 (Demiris, Afrin et al. 2008). 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 conditions. 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.

Recently, 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 (Bliemel and Hassanein 2007). The Ontario *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 (MOHLTC 2007)—which would necessitate the flow of health information from healthcare institutions and practitioner offices to patients and community care providers, and in the 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 (CHI 2007a) and the recent announcement of the goal for every resident of Ontario to have an electronic personal health record (PHR) by 2015 (MOHLTC 2008). 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 broad literature review (Dorr, Bonner et al. 2007) of 109 articles covering 112 PHR system descriptions, 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 report is to discuss certain issues concerning the general implementation of electronic personal health records. In this paper, Section 2 presents a discussion of possible PHR architectures that have been proposed, pilot tested, or implemented. Section 3 discusses security and privacy issues that affect the design and operation of PHRs, Section 4 compares some of the attributes of different PHR architectures, and Section 5 is a concluding discussion of the findings of this study.

PHR SYSTEM ARCHITECTURES

To accomplish the goals of a PHR to improve healthcare, there is a suggested minimum of information it should include (Tang, Ash et al. 2006). From the patient, both subjective and objective information are expected. The former should include a medical history, descriptions of events, and detailed listings of symptoms. The objective measurements could include home measurements of data such as blood pressure, blood sugar levels, and weight. Additional technical capabilities are available through medical equipment at home for automated data upload and compliance validation. Healthcare practitioners, in particular family doctors, would provide specific EMR data—or EHR data in the case of a practitioner primarily associated with an institution—as well as notes on visits and test results, and referral information for alternate or specialist practitioners. Institutions would be expected to include their EHR data, results of tests or other relevant data—imaging results, or video as suggested for behaviour observation (Oberleitner, Elison-Bowers et al. 2007)—notes on treatments or observations, and historical data such as prescriptions, visit dates, and future appointments (Oh, Sheble et al. 2006).

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.

Tethered PHR: 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.

Standalone PHR: At the other end of the continuum, a 'standalone' PHR may take on several forms. We will describe two of the more likely ones:

a) Smartcard PHRs are systems where patient data is stored on some portable media such as a smartcard, supported by software that can be accessed by computers 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 being rolled out to 85 million German citizens (Gesundheitskarte 2008)). However, there is little protection from loss, theft, or damage (Tang, Ash et al. 2006), 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 (Wright and Sittig 2007). Standalone PHRs may also be primarily patient driven, in which case they are not 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 (Tang, Ash et al. 2006). However, if they are state developed and sanctioned, with proper security and privacy controls, as in the smartcard system currently being implemented nationally in Germany (Gesundheitskarte 2008) they may be regarded as trusted PHRs by both institutions and practitioners.

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 treated or examined and where electronic records of the engagements have been maintained. Commercial portals that support patient-driven consolidation (Gunter and Terry 2005) 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 of clinical records from well-known systems or to aid in identifying the correct or relevant information in the health file (Kim and Johnson 2004).

Integrated PHR: 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 (Tang, Ash et al. 2006); 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 (Gunter and Terry 2005). 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 (Gunter and Terry 2005). 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. The architecture without a central repository 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 (InterSystems 2008). Integrated systems are generally implemented as portals with either secure Internet access (Ueckert, Goerz et al. 2003) or dedicated kiosks (Jones 2003). Additional functionalities may be offered, such as terminology translation or definitions, video attachments for remote diagnosis, or biometric—e.g., blood pressure, or blood glucose monitoring and tracking (Berner and Moss 2005; Lee, Delaney et al. 2007; Oberleitner, Elison-Bowers et al. 2007).

Other PHR models have been proposed to deal with the diverse nature of health data and distributed sources of data, including a subscription model. In this model (Mandl, Simons et al. 2007), 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 (Young, Mintz et al. 2004; Cooke, Watt et al. 2006) 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 (Oberleitner, Elison-Bowers et al. 2007). Medication renewals and alerts can provide feedback on compliance to the prescribing physicians (Wang, Marken et al. 2005). 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 (Ueckert, Goerz et al. 2003) 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.

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 (HarrisInteractive 2008), 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 (CHI 2007b). 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 (Clarke and Meiris 2006; Croll and Croll 2007). Systems can be encrypted and password protected, but that is not necessarily sufficient in the case of bad systems or poorly chosen passwords (Wright and Sittig 2007). 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 (Tang, Ash et al. 2006). 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 (Simons, Mandl et al. 2005). 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 (Ueckert, Goerz et al. 2003). For example, Enterprise Master Patient Registries (EMPIs) (Sobun 2000) have been developed in a number of Canadian jurisdictions. These 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 (Mandl, Simons et al. 2007). In the separation of functions approach, different functional tasks are performed on separate systems, 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 (Mandl, Simons et al. 2007). 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 (Mandl, Simons et al. 2007).

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 (Simons, Mandl et al. 2005). One of the key concerns is unauthorized access (Win, Susilo et al. 2006), which can be prevented by proper authentication. Authentication is traditionally a username or ID with an associated password, but these have been superseded by other, more robust methods (Sax, Kohane et al. 2005). 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 (Sax, Kohane et al. 2005). If one focuses on the physical location as one of the parts of authentication, then that could limit 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 (Mandl, Simons et al. 2007). 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 (Mandl, Simons et al. 2007).

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 (Baker and Masys 1999), 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 (Baker and Masys 1999). However, not all encryption is good encryption (Wright and Sittig 2007) 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 (Wright and Sittig 2007) 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

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

(Sax, Kohane et al. 2005) in the case of 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, it 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 (Agrawal and Johnson 2007), so that those responsible for the patient's care can perform efficiently.

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 each class of user, or to specific users (Baker and Masys 1999; Agrawal and Johnson 2007). 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 (Baker and Masys 1999); 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. However, an emergency room physician could easily find the current list of medications and prior history of a patient in order to deliver the appropriate health care with reduced risk (Ueckert, Goerz et al. 2003). 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 (Mandl, Simons et al. 2007). These rules have been implemented at the business logic level in *Indivo* (Mandl, Simons et al. 2007) or at the database access level (Agrawal and Johnson 2007).

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 (CHI 2007a). 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 (CHI 2007a). 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 (MOHLTC 2004). 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 place, but if the data is 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.

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 short 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, including complexity, access, data sources, major risks, security and privacy, and finally some Web sites where example installations or trials are described. 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. Several of these systems from different vendors are under trial at 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. There are currently no standard EMR record and application specifications in Canada (shortlists of acceptable commercial EMRs, some containing dozens of systems, are maintained in each province). 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, 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 large networks and systems requires high-level collaboration	Smartcard: Loss or theft of device; Each provider requires standards to link to smartcard. Consolidator: Non-standard data sources and consumer IDs to be accommodated; Privacy on these systems not protected by HIPAA[2] (U.S.); Extra-territorial access by U.S. government
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 (Chan 2008)	U.S. DVA (InterSystems 2008)	Smartcard: Germany (Gesundheitskarte 2008) Consolidator: HealthVault (Anonymous 2008)
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

[2] HIPAA – Health Insurance Portability & Accountability Act - Federal U.S. act that governs U.S. healthcare privacy.

The Standalone Smartcard architecture has received little attention in North America but is currently being rolled out in Germany. This is expected to generate a significant amount of evaluation data as its implementation continues over the next few years. Although it is conceptually simple and highly portable, being similar to chip and PIN bankcards, these smartcards will contain a large amount of sensitive information (obviously requiring encoding at a high level) and will be susceptible to theft and loss. Security will be more difficult to maintain at the necessary level, and network backup facilities will be needed in case of theft or loss.

The Standalone Consolidator architecture has been developed into commercial products by several major U.S. firms who currently have several U.S. sites under trial, one at a major clinic (Lohr 2008) and another at one of the largest U.S. Health Maintenance Organizations (HMOs) (Anonymous 2008). 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. 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 given the appropriate level of attention. Unfortunately, there are major privacy concerns about standalone consolidators. At this point they are not covered in the U.S. by HIPAA[3] (Health Insurance Portability & Accountability Act). This could mean in the extreme that data collected on these systems could be sold to other firms for a variety of uses, such as data mining, marketing, etc. Installations of these systems by U.S. firms in Canada could allow unrestricted access to private information by the U.S. government under the U.S. Patriot Act.

DISCUSSION

In general, patients want to be able to access and control their own health records through online access (Denton 2001; Adler 2006). 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 (Staroselsky, Volk et al. 2006). Second, for chronically ill patients, many studies have shown that the PHR is a contributing factor in positive outcomes, with a notable correlation between active PHR use and health outcomes (Dorr, Bonner et al. 2007). 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 (Earnest, Ross et al. 2004) have been cited. For example, 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 that they are in less than perfect health (Staroselsky, Volk et al. 2006).

[3] http://www.hhs.gov/ocr/privacy/index.html

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 (Hampshire, Blair et al. 2004). 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, 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 such as educational content. Many patients are very 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 (Earnest, Ross et al. 2004).

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. A matter of great importance to Canadians 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 for some time to be a significant barrier to general adoption of PHRs in Canada.

REFERENCES

Adler, G. K. (2006). "Web Portals in Primary Care: An Evaluation of Patient Readiness and Willingness to Pay for Online Services." J Med Internet Res **8**(4): e26.

Agrawal, R. and C. Johnson (2007). "Securing electronic health records without impeding the flow of information." International Journal of Medical Informatics **76**(5-6): 471-479.

Anonymous (2008). Microsoft Healthvault scores big win: Pilot with Kaiser http://www.networkworld.com/community/node/28560 (Jan 7 2009). Network World.

Baker, D. B. and D. R. Masys (1999). "PCASSO: a design for secure communication of personal health information via the internet." International Journal of Medical Informatics **54**(2): 97-104.

Berner, E. S. and J. Moss (2005). "Informatics Challenges for the Impending Patient Information Explosion." Journal of the American Medical Informatics Association **12**(6): 614-617.

Bliemel, M. and K. Hassanein (2007). "Consumer satisfaction with online health information retrieval: A model and empirical study." e-Service Journal **5**(2): 53-83.

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

Chernos, S. (2007). "Cross-country check-up." Technology for Doctors (October 2007).

CHI (2007a). 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). Montreal, Canada Health Infoway.

CHI (2007b). 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). Executive Summary, Canada Health Infoway.

Clarke, J. L. and D. C. Meiris (2006). "Electronic Personal Health Records Come of Age." American Journal of Medical Quality **21**(3): 5S-15S.

Cooke, T., D. Watt, et al. (2006). "Patient expectations of emergency department care: phase II – a cross-sectional survey." Canadian Journal of Emergency Medicine **8**(3): 148-57.

Croll, P. R. and J. Croll (2007). "Investigating risk exposure in e-health systems." International Journal of Medical Informatics **76**(5-6): 460-465.

Demiris, G., L. B. Afrin, et al. (2008). "Patient-centered applications: Use of information technology to promote disease management and wellness." Journal of the American Medical Informatics Association **15**(1): 8-13.

Denton, I. C. (2001). "Will Patients Use Electronic Personal Health Records? Responses from a Real-Life Experience." Journal of Healthcare Information Management **15**(3): 251-9.

Dorr, D., L. M. Bonner, et al. (2007). "Informatics Systems to Promote Improved Care for Chronic Illness: A Literature Review." Journal of the American Medical Informatics Association **14**(2): 156-163.

Earnest, M. A., S. E. Ross, et al. (2004). "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 **11**(5): 410-7.

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

Gunter, D. T. and P. N. Terry (2005). "The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions." J Med Internet Res **7**(1): e3.

Hampshire, A. J., M. E. Blair, et al. (2004). "Variation in how mothers, health visitors and general practitioners use the personal child health record." Child: Care, Health and Development **30**(4): 307-316.

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

InterSystems (2008). 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.

Jones, R. (2003). "Making health information accessible to patients." Aslib Proceedings **55**(5/6): 334-338.

Kim, I. M. and B. K. Johnson (2004). "Patient Entry of Information: Evaluation of User Interfaces." J Med Internet Res **6**(2): e13.

Lee, M., C. Delaney, et al. (2007). "Building a personal health record from a nursing perspective." International Journal of Medical Informatics **76**: S308-S316.

Lohr, S. (2008). Google health begins its preseason at Cleveland Clinic http://bits.blogs.nytimes.com/2008/02/21/google-health-begins-its-preseason-at-cleveland-clinic/?ref=technology (Jan 16 2009). New York Times. New York, NY.

Mandl, K. D., W. W. Simons, et al. (2007). "Indivo: a personally controlled health record for health information exchange and communication." BMC Medical Informatics and Decision Making **v7** (25): 1-10.

MOHLTC (2004). Personal Health Information Protection Act: An Overview for Health Information Custodians (Ministry of Health and Long Term Care). Toronto, Queen's Publisher.

MOHLTC (2007). Aging At Home Strategy Backgrounder: Ministry of Health and Long Term Care. Toronto, Queen's Publisher.

MOHLTC (2008). 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.

Oberleitner, R., P. Elison-Bowers, et al. (2007). "Optimizing the Personal Health Record with Special Video Capture for the Treatment of Autism." Journal of Developmental and Physical Disabilities **19**(5): 513-518.

Oh, S., L. Sheble, et al. (2006). "Personal pregnancy health records (PregHeR) Facets to interface design." Proceedings of the American Society for Information Science and Technology **43**(1): 296-296.

Sax, U., I. Kohane, et al. (2005). "Wireless Technology Infrastructures for Authentication of Patients: PKI that Rings." Journal of the American Medical Informatics Association **12**(3): 263-268.

Simons, W. W., K. D. Mandl, et al. (2005). "The PING Personally Controlled Electronic Medical Record System: Technical Architecture." Journal of the American Medical Informatics Association **12**(1): 47-54.

Sobun, C. (2000). "EMPI allows networks to integrate medical records." IT Health Care Strategist **2**(7): 10-13.

Staroselsky, M., L. A. Volk, et al. (2006). "Improving electronic health record (EHR) accuracy and increasing compliance with health maintenance clinical guidelines through patient access and input." International Journal of Medical Informatics **75**(10-11): 693-700.

Tang, P. C., J. S. Ash, et al. (2006). "Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption." Journal of the American Medical Informatics Association **13**(2): 121-126.

Ueckert, F., M. Goerz, et al. (2003). "Empowerment of patients and communication with health care professionals through an electronic health record." International Journal of Medical Informatics **70**(2-3): 99-108.

Urowitz, S., D. Wiljer, et al. (2008). "Is Canada ready for patient accessible electronic health records? A national scan." BMC Medical Informatics and Decision Making **8**(1): 33.

Wang, C. J., R. S. Marken, et al. (2005). "Functional Characteristics of Commercial Ambulatory Electronic Prescribing Systems: A Field Study." Journal of the American Medical Informatics Association **12**(3): 346-356.

Win, K. T., W. Susilo, et al. (2006). "Personal Health Record Systems and Their Security Protection." Journal of Medical Systems **30**(4): 309-315.

Wright, A. and D. F. Sittig (2007). "Encryption Characteristics of Two USB-based Personal Health Record Devices." Journal of the American Medical Informatics Association **14**(4): 397-399.

Young, A. S., J. Mintz, et al. (2004). "A network-based system to improve care for schizophrenia: the medical informatics network tool (MINT)." Journal of the American Medical Informatics Association **11**(5): 358-367.

McMaster University
1280 Main St. W. DSB A201
Hamilton, ON
L8S 4M4

Tel: 905-525-9140 ext. 23956
Fax: 905-528-0556
Email: ebusiness@mcmaster.ca
Web: http://merc.mcmaster.ca