PERSONAL HEALTH RECORDS IN CLOUD COMPUTING

Priyanka R. Padol[1], Harshada K. More[2], Nutan V. Mandre[3], Pooja N. Shimpi[4]

[1,2,3,4] *Student of computer Engineering, GESRHS college of Engg., Nashik, Maharashtra, India*

---***---

Abstract - *Personal health record (PHR) is considered a crucial part in improving patient outcomes. However the adoption rate by the general public in the US still remains low. To find out the barriers in adopting PHR, we have surveyed articles related to personal health record system (PHRS) from 2008 to 2016 and categorized them into 6 different categories such as motivation, barriers, ownerships, interoperability, privacy, and security and portability. To achieve fine-grained and scalable data access control for PHRs, we are useing attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multiauthority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of our proposed scheme.*

***Key Words*: Personal Health Record, Barriers in PHR adoption, Dublin Core Metadata, Cloud based PHR, PHRS architecture, HL7 CDA, Standard Medical Codes , cloud computing, data privacy, fine-grained access control, attribute-based encryption.**

1.INTRODUCTION

Personal Health Record is defined as "an electronic, lifelong resource of health information needed by individuals to make health decisions". PHR acts as an important intermediary between physicians and patients . The main goal of PHRS is to enable patients to manage and maintain their personal health records as well as improving healthcare delivery and reducing cost. PHRS is often provided to consumers by their employers, health providers, health insurers, or independent vendors . Some of the PHR models are: first, a standalone model where the data is stored in the "consumer's computer or the Internet and is often used to track and monitor health related behaviors, such as exercise and diet". Second, tethered PHR that allows communication with EHRs to share data from multiple healthcare sources. It also offers many features such as email, reminders, and scheduling to support care management by updating and providing accurate information which benefits both users and healthcare providers. Another type of PHRS is called interconnected PHR system which supports collaboration with other health record systems (e.g. EHR, EMR etc.). PHRS have been implemented successfully for many years in many countries such as Australia, Netherlands and Germany but in the U.S., it is still struggling. Some of the issues are financial, interoperability, security, and privacy. The adoption of PHR is still at a low rate than it supposed to be in the USA. In this paper, we are trying to find out the barriers in adopting PHRs and to propose a potential solution that can promote the adoption of PHRS by general public so it is possible to implement continuity of care in community settings, evidence based care, and also prevent potential medical errors from the lack of clinical information. The paper is organized as in the following: background and aspects of PHRS, system structure of PHRS, proposed solution, and conclusion.

2. BACKGROUND AND CATEGORIES OF PHRS

2.1. Motivation

In this section, we identify some of the features and benefits of PHRS that could motivate people to adopt PHRS. PHRS offers many benefits including: (1) improving healthcare quality (e.g. continuity of care, having their records anytime and anywhere, etc.); (2) improving the relationship between patients and physicians; (3) saving cost and time (e.g. by avoiding repeated tests), (4) improving privacy (e.g. patient can control their own health records and share them with whom they want); (5) increasing patient safety (e.g. during the emergency); (6) empowering patients to take charge of their health, etc.; and more importantly, it will mitigate and prevent medical errors.

PHR mostly used by "patients with chronic conditions, frequent users of healthcare, caretakers of elderly patients" and older patients . Both younger and older people can get benefits from adopting PHR. However, older people "tend to be late adopters of technology and may be hesitant to adopt a PHR if the benefits are not made clear", i.e., the barrier is higher for those who are in need.

Some of the motivating features of PHRS are: tracking chronic conditions, storing health information of their family, sharing health records with physicians and family, drug interactions checker, finding a doctor covered by their insurance network, reference information from trusted sources, uploading medical documents and uploading information from multiple medical devices, accessible by authorized users, and keeping health data secure and private . Other motivating features of PHRS are presented by Fricton and Davies including: organizer of health records, calendars and reminders features, health education, communicating with physicians and health plan providers, accessibility to community services, managing healthcare cost, accessibility online, and easy access to their own medical records.

Another study by Sunyaev et al. identified 25 end-user features for successful PHR implementations including: online accessible, up-to-date medical information, presented in a cognitively accessibility way, editable by patients and correctible by physicians, technically accessible, controllable by patients, accessible in case of emergency, traceable, capturing cost information, printing documents, secure messaging, prescription refills, appointment scheduling, reminders, notifications, educational information, support groups, device integration, decision support, filing referral requests, medicine information, address book, quality, localization, and searchability. Interoperability is also an important factor of the adoption of PHRS. Health risk assessment, as suggested by Center for Disease control and prevention (CDC), can provide health awareness to the general public by providing their "as-is" health condition. Sample paragraph, The entire document should be in cambria font. Type 3 fonts must not be used. Other font types may be used if needed for special purposes. The entire document should be in cambria font. Type 3 fonts must not be used. Other font types may be used if needed for special purposes.

2.2. Usability

In this section, we identified factors that cause the slow adoption of PHRS. Pushpangadan, et. al. specified many themes including:

- Features: lack of necessary functions that allow patients to access their medical records and their family members, make appointments, reminders, prescriptions, refills, referrals, get test results, find educational resources and communicate with providers for allergies, immunizations, emailing physicians, accessing medical reports, and tracking their health conditions

- Usability: Some of PHRS users find it easy to use but they had to face a difficulty of understanding medical terminology and inaccurate information.

- Communication: adoption of PHRS does not necessarily enhance the communication between patients and health providers.

- Digital divide: refers to the skills such as Internet access, computer technologies, and medical devices that patients may not have.

- Medical terminology: Most people have difficulty in understanding medical terminology. Therefore, the medical terminology should be kept as basic as possible or at least offering medical training to overcome such challenges. Security and privacy also are big concerns by patients.

Pak and Song proposed a framework called Health Capability Maturity Model (HCMM) to assess individual's health based on their health maturity level. This model can be used as a roadmap to help individuals to improve their health by assisting them to achieve desired maturity-level so they can adopt a PHRS and take control of their health and medical record keeping. The health maturity levels are described as shown in table 1. We also applied these levels to the adoption of PHRS as shown in table 1 below.

Table 1: Health Capability Maturity level and the use of PHRS

HCMM Level	Individual's perspective of their health	PHRS adoption
Level 0	Lacking of: -Health self-management -Health Knowledge -Motivation	Not using PHRS
Level 1	-Awareness of the necessary changes -Willing to change to improve their health	Considering PHRS but not adopting it yet
Level 2	Take actions on: -Adopting some healthcare plan -Making decision related to their health management	Slow adoption of PHRS
Level 3	Use of quantitative techniques to: -Self-monitoring -Control performances	Use of some features of PHRS
Level 4	-Proactive rather than reactive -Respond quickly to the health changes and improvement opportunities	Quantitatively monitor and control their health using PHRS

Krist, A. et al, found that patients can be effectively engaged in using PHRS in small to medium-sized primary care practice settings where most patients receive their care. Another study by Price et al found that seven chronic diseases - asthma, diabetes, fertility, glaucoma, HIV, hyperlipidemia, and hypertension – can benefit from having PHR enabled self-management plans. Another paper compared Google health and Microsoft Health Vault PHR systems on five dimensions - usability, utility, security, privacy, and trust - and found that user experienced difficulty in using these systems including entering medical information, navigating records, a busy screen, adding details and understanding medical terminology . In this study, Google health was rated higher on the dimensions of ease of use and utility while Microsoft HealthVault was rated higher on the dimensions of privacy and trust. Similar study by Archer et al. conducted a literature review on various aspects of PHR such as design, functionality, implementation, applications, outcomes, and benefits. They found some factors that make consumers reluctant to use and implement PHR. Those include lack of consumer involvement during the development processes (e.g. planning, design, and implementation of PHR system); lack of trust in the provider, security, health literacy, technology literacy, accessibility, awareness; lack of ability in physical, cognitive; usability and socio cultural influences; and uncertainty on ownership, transportability, and research on the utility and features needed by consumers.

Similar barriers were identified by other studies. Some barriers on provider tethered PHRS, studied by Vydra, et al., were including the lack of reimbursement for the time physicians spent in portal communication, change of workflow, and resultant change resistance. They suggested that in order to encourage physicians to use PHRs: offer rewards, provide financial reimbursements for the time spent on PHRS, and provide support on staff assistance and training. Other issues in PHRS adoption are the interoperability with electronic medical records and use by healthcare providers .

2.3. Ownership

In this section, we identify the providers of the PHRS and issues related to their systems. There were 117 vendors of PHRS as of July 2010 and 600 vendors of EMR as of July 2011. Most of them offer their services for free or at a little cost . With these many platforms, there is a need to establish a global standard for medical records in order to exchange data among different health systems (e.g. EHR, PHR, MHR); otherwise these systems will not be valuable because they will not meet the patient, physician, care providers, etc. expectation and needs. This in turn will reduce the use of these systems especially PHRS. The tethered PHRS type has been developed by many commercial PHR platforms such as Microsoft Health Vault, Google Health, CBSHealthWatch's, Dossia (ww.dossia.com), MyGroupHealth (www.ghc.org) etc.. However, even large companies such as Microsoft Health Vault and Google Health services are not available outside the United State. This can limit the use of their PHR systems to the people who are travelling outside the U.S. In addition to that most of PHR systems do not offer built-in emergency access to the record except thirdparty services available for HealthVault. Also both services do not offer feature like the ability to search within patient records and provide user interface other than in English.

In January 1, 2012, one of the biggest PHR providers, Google, stopped its Google Health™ System and asked their registered patients to retrieve and transfer their files to their computers, other PHRS vendors, or to their physicians by January 1, 2013. Brandt and Rice identified 22 possible reasons for the Google Health™ disconnection including themes of policy, trust, marketing, financial reasons, planning and implementation, user cap- ability, and appeal . Since Google Health is no longer in service, this raises an important question - would that be possible for Microsoft Vault or other PHRS provider to discontinue their services as well?. Patients do not have much trust on the availability and accessibility on their own PHRS offered by a company. Companies may discontinue their services of PHRS (e.g. Google Health) at any time due to many reasons such as going out of business. Therefore, it will be better and secure to have stand-alone PHRS. In this case, there is a need to build a stand-alone PHRS that can be controlled by individuals based on rules for both individuals and physicians in order to make a comprehensive PHRS that can be trusted and valuable for all parties. This can be done by securely storing their clinical data in the clou based repository and follow the international standards such as HL7 standard in order to be interoperable with EHR. We also suggest that separating the clinical data from applications which will give the users more freedom by not limiting themselves to one provider or an application. This in turn enables users to access and modify their clinical data anytime and anywhere from any portable devices. In this case, users' clinical data such as medical history can be secured even when PHRS provider discontinue their service for whatever reasons (e.g. Google Health). It will also leave the users with more options and choices, which in turn will motivate people to adopt and use PHRS. Consumers' clinical data will be stored in the cloud based repository using medical format and code standards:

- Medical codes: SNOMED CT, ICD-10, LOINC, DICOM etc.
- Document format: HL7 CDA • Metadata: Use of Dublin Core.

The proposed concept is illustrated in the Fig. 1. In the figure, the content of each HL7 CDA document is described in doubling core (DC) for easy retrieval.

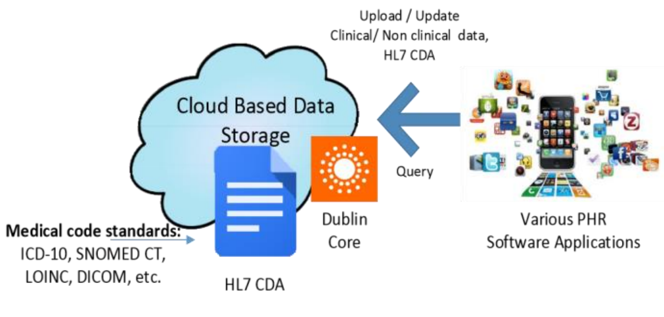

Figure 1. Use of standards and Separation of data from PHRS

2.4. Interoperability

In this section, we discuss one of the big issues that hinder information exchange among different healthcare systems. Personal Health Record System (PHRS) and Electronic Health Record (EHR) are independent systems with the purpose of providing the right clinical information to the caregivers at right time to ensure quality care while allowing patients to monitor their own health. In PHRS, patients have full control over their PHRs. However, in PHRS, patients are concerned about their clinical data privacy and are not willing to share their health data with others, which makes it difficult for doctors to provide them the right treatment especially in emergency situations. According to the Institute of Medicine "poor communication and exchange of medical information at transition points for patients from one provider to another are responsible for many medical errors and adverse drug events". According to the Healthcare IT news, preventable medical error is considered to be the third killer after heart disease and cancer in the US which cause the death rate of 400,000 people each year. From the patient perspective, there is no systematic way to share their clinical data in the PHR with their physicians due to reliability concern. On the other hand, in EHR systems, the data can be shared with many related agencies (e.g. insurance companies, pharmacies, etc.) each of which keeps a part of the patients' records based on their specialties. However, EHR systems are developed by independent vendors and designed to meet their customers' needs. This in turn causes interoperability issues that hinder data exchange between PHRS and EHRS and even between EHRS that were developed by different vendors.The interoperability issues include: data definition (e.g. vocabularies mismatching, size, name, etc.), change of workflow (e.g. new processes, lack of currency, lack of interoperable software, etc.), security and privacy (e.g. authorizing access, data quality, etc.).

The major concern from the clinicians' point of view was "the integration and standardization" in order to share data by multiple care providers. Pringle et al. proposed a technical implementation guide for connectivity between PHRs and EHRs that can help overcome the interoperability issues by creating a set of agreements that are approved and supported by all participants. This approach looks to the resolution of technical concern from the national collaborative efforts, including:

- The Healthcare Information Technology Standards Panel (HITSP) to enable integration between systems in order to share information.
- Integrating the Healthcare Enterprise (IHE) which "is a global initiative that creates the framework for passing vital health information seamlessly - from application to application, system to system, and setting to setting - across multiple healthcare enterprises.".
- American Health Information Community (AHIC).

A study by Kaelber and Pan compared the potential value of PHR systems (e.g. provider-tethered, payer-tethered, third- party, and interoperable PHRs) in the United States. They found that interoperable PHRs show the most value, followed by third-party PHRs and payer-tethered while provider-tethered shows negative net value . "As both EHRs and PHRs become standardized, patients will be able to move from one place to another and have their medical records accessible and transferable wherever they go" . The structural standards of PHRS include: Continuity of Care Document (CCD), ASTM Continuity of Care Record (CCR), Clinical Document Architecture (CDA), Digital Imaging and Communications in Medicine (DICOM), Good Electronic Health Record (GEHR), Health Level Seven (HL-7), International Classification of Diseases (ICD-9/ICD-10), Systemized Nomenclature of Medicine (SNOMED), and Vocabularies contained in the Unified Medical Language System (UMLS). However, incorporating these standards into hospitals' existing systems is challenging because many of them need re-engineering or start from scratch. For large PHRS provider like Microsoft there are not major technical barriers to entry, but without adopting data standards for interoperability it will be challenging to import and combine data in a meaningful way. Health record systems (PHR, EHR, etc.) should take advantage of and/or learn from other information technology successes in other fields (e.g. Apple). "An essential first lesson is that ideally, system components should be not only interoperable but also substitutable" . PHRS can be used as the central piece of health information exchange to overcome interoperability issues among different healthcare providers . Having interoperable health data in place, "the patient's PHR can be achieved with a simple, inexpensive, and expedient process." . However, these studies basically suggest for all participants to follow standards that already available to overcome interoperability issues but they did not mention how to make the PHRS and EHR interoperable in practices. To overcome interoperability issues that hinder exchanging of health data between different healthcare organizations, DePalo et al. applied enterprise architecture principles during the implementation of Integrating Healthcare Enterprise (IHE). Most of existing EA models (e.g. TOGAF, FEA, Zachman, Gartner) focus on aligning business functions, objectives, and goals with IT within organizations but poorly focused on supporting interoperability externally with other organizations. Therefore, DePalo and Song proposed an approach to leverage the existing EA models by adding an interoperability layer that can deal with external entities since information is needed to be shared among external health organizations (e.g. Hospital A, Hospital B, pharmacies, radiology, laboratories, etc.).

2.5. Privacy and Security

Security and privacy are the main concern for patients in regard to their health records. According to Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), patients have the right to access and get a copy of their health records although it does not specify the exact manner in which the access is to be given . In addition, all of healthcare systems (e.g. PHR, EHR, etc.) must be adhered to HIPAA regulations including security, privacy, transmission, and releasing patient's medical information. However, compliance to the regulations related to privacy and security may enact more barriers for the organizations to deploy such systems (PHRS, EHRS, etc.). But how to make PHRS compliant to HIPAA in technical aspect is still an ongoing research issue. Furthermore, security and privacy are considered one of the issues that hinder the sharing of health data among EHRS and between PHRS because the clinical data cannot be shared unless authorized by patients . Liu et al. found that patients trust downloadable applications more than websites to put their health records. In addition, patients feel safer using paid services rather than free services for their PHRS. Another study also found that people preferred using PHRS from strong brand company (e.g. Microsoft, and others.) for the similar reason.

2.6. Portability

Portability is an important aspect of building PHRS as stated in the following: "Portability is an U.S. employee's right to keep or maintain certain benefits when switching condition where quick decisions must be made, etc.). Therefore, it is important for consumers to have portable records that can go with them as they move across and within the healthcare system in order to improve continuity of care. But for the most part, current PHRs do not offer this capability. Therefore, devices including cellphone, computers, tablet, sensors, etc. that users are using to monitor their health must be portable to PHRS . As discussed in, the medical data should not be intercepted and eavesdropped during the data transmission through wireless network. The use of multiple layers of complex defense mechanism may help promote the security of medical data. Exchanging information between healthcare systems is facilitated by the adherence to the medical document standards. The HealthVault takes the lead by supporting both Continuity of Care Record (CCR) (created by the ASTM) and Continuity of Care Document (CDR) (created by HL7.

Another paper presented an integration the Healthcare Enterprise (IHE) profile to overcome interoperability issue of transporting medical and sharing information between healthcare providers by utilizing distributed computing technologies such as SOAP envelopes for ebXML over mobile networks. They used networks known as Health Information Exchanges (HIE) and the National Health Information Network (NHIN) to make the interactions between transport facilities possible. For querying, receiving, updating and sending medical records in the transport environment, DePalo et al. leveraged the advantages of ebXML using registries and repositories in mobile networks. Electronic business XML (ebXML) is a standard that uses XML based-message to exchange business data globally in a secure way but it is also successfully applied to transport medical data. The summary of the section 2 is shown in the Fig. 2 and the table 2.

Figure 2. Barriers in PHRS adoption

Table 2. Summary of Barriers of PHRS adoption

Category	Barriers	Proposed solution
Usability	-Technology literacy - Lack of user involvement - New workflow - Change resistance	- Training support - Guide users through available resources - Involve users from the beginning
Ownership	Lack of trust in the provider	Separate data from application
Interoperability	Lack of interoperability	Impose standards
Privacy and Security	- Hacking - Unauthorized access - Lack of trust	-HIPAA regulation -Encryption and decryption - Time stamp -Control access
Portability	- Lack of accessibility - Lack of transportability	Separate data from applications
Motivation	- Awareness of PHR value - Health literacy	-Health risk assessment -Reward offering for use -Reimbursement for the physician time for portal

3. PHRS ARCHUITECTURAL STYLES

The architecture of PHR is based on National Institute of Standards and Technology architectural (NIST) model, which "provides a description of how it addresses the storage, management and access of its health data". Steele et al. identified five existing PHR architectures but in our classification we used four categories including: USB or other portable storage-based PHR, smartcard-based PHR, mobile device-based PHR, a web or cloud -based PHR. The explanation, providers, advantages and disadvantages of these PHR architectures are summarized in table 3.

Table 3: Summary of PHRS Architectures

PHRS Architecture Type	Description	Advantages	Disadvantages
USB or other portable storagebased PHR (e.g. SD card) - These devices are commercially available	This type consider as Stand-alone PHR (e.g. USB, Secure Digital (SD)).	Portable Accessible - No need for network connection Data kept secure and private (by using encryption /decryption methods)	-Need concomitant devices for connection with other devices - Required interoperable interface for exchanging data - Small storage - Can be lost or damaged
Smartcard-based PHR. -Providers include: American Medical	-This type also consider as a Stand-alone PHR -"A portable integrated circuit (IC) chip-based	No need for network connection to access data It helps in emergency	-Need for network connection. Lack of data sharing -Need reader devices
Association Health Security Card pilot; Lake Pointe Medical Center LifeMed Smart Card; Memorial Hospital LifeMed Smart Card, etc.	plastic card (smartcard) can either store an individual's health data physically or under a logical file system" .	situations by storing important data (e.g. blood type, known allergies and immunization record) - Easy to use - Small size/ Carry-able - Secure - Portable medical record	Need middleware to exchange data securely - Can be lost easily No desired control access (e.g. authorized person can access all data) - Virus concern from helath providers point of view
Mobile device based PHR -Numerous mobile apps Commercially available	This type mostly considered as a Stand-alone PHR but can be webbased Smartphone or tablet can be used as local data repository may have connection to cloud data repository	Wireless connection Real time access Provide dynamic data management or update doctors can get instant updates on patients' concerns	-Less secure while using wireless connection and slow connection - Limited data sharing with external parties Users responsible for backing-up their data interface with EHRs limited
A web-based /cloud-based PHR -provider include: Independent vendors (e.g. Dossia, MyGroupHealth, My HealtheVet, Health Vault and MyChart)	- Combining standalone, interconnected and tethered PHR.	-Need of only web browser - Maintenance and upgrading are done by providers -Accessibility -Help in the integration sharing, and recovery of data.	- Lack of breakglass access in case of emergency situation -Providers may discontinue their service of PHRS for whatever reasons (e.g. Google Health) Interoperability and integration problems.

To ensure security and confidentiality in the cloud computing, Dhivya, et al. proposed encrypting the data before it reaches the server in order to avoid internal hacking. Barouti, et al. proposed a protocol that allows health organizations to produce statistical information about encrypted PHRs stored in the cloud. Their protocol depends on two homomorphic cryptosystems: Goldwasser-Micali (GM) and Paillier. The queries are executed on K_d-tree from encrypted health records. This protocol ensures privacy of both health organizations and patients.

Fox, et al. proposed the use of Mashups to create a virtual personal health record where a patient and care provider can collaborate using trusted social network. This in turn can overcome issue of using centralized data store of PHR by making the data sharable between the patient and care providers. Genitsaridi et al. suggested the basic requirements for creating an intelligent PHR system: make the system as a free open source system where it will be available to the worldwide community, make the system as a web-based system, make the system compliant to high quality functional standards and make the architecture maintainable, expendable and interoperable.

Ontology-based approaches have been proposed by other researchers to enable semantic interoperability by searching among a large number of electronic CDA documents of a patient and providing quick access to relevant and meaningful information instead of searching entire documents in the EHRs. Patel et al. built a system called TrialX on top of PHR to enable patients to match their health condition to clinical trials. This system extended search parameters compared to ClinicalTrials.gov (search by keywords only) where a patient can search by keywords and demographics (e.g. age, gender, city and study site). The return results can be reduced to relevant information using semantic web technologies.

4. PROPOSED ARCHITECTURE

4.1. Scenario

D.J. is a 73-year-old white male with a history of diabetes who lives in Los Angeles, CA. He was getting his diabetes medicine from a local CV pharmacy as referred by his doctor.Three years ago, he was hospitalized for three days at one of the hospitals in Los Angeles, CA due to a broken leg and found out that he has a kidney problem and needs to be referred to a specialist as soon as possible, otherwise it will cause kidney failure. He went to a specialist as recommended and went through many treatment procedures including a physical exam, lab test and radiology. When the results came out, they found out that his kidneys have failed and that he needs dialysis every other day. D.J used a mobile application called the personal mobile health record system (PMHRS) to collect all of his health records in HL7 CDA since hospitalization. He also used the cloud uploader to upload these records into his cloud storage, so they can be accessible from anywhere at anytime. For the non-standard data format such as a scanned document, he used Dublin Core meta file to describe what the document is about, so it can be retrievable later on.

D.J. moved to Maryland State to live with his son. Two months later, he was unconscious due to a heart attack, so his son took him to the emergency room. While he was in the hospital, the physician wanted to give him a drug, but his son provided the access to his father's health records in the cloud to the physician. When the doctors checked his health records, he found out that the drug would cause an allergic reaction and could put his life in danger. Therefore, the physician gave him another drug that does not have such reaction. Also, D.J did not have to re-do the physical examination, lab tests, radiology, etc. because all of his health records were in the cloud.

4.2. Prposed Solution

As discussed in Section 2, there are a number of barriers for PHRS. In an attempt to lift such barriers, we are proposing a hybrid PHRS (as shown in Fig. 3) that consists of:

- Consumer's clinical data collection module: we have built a mobile application called personal mobile health record system (PMHRS) to collect clinical data and observed symptoms in standard codes.
- Cloud uploader: we have built a web based application that can upload various types of files including HL7 CDA, Dublin Core metadata, DICOM, and any other documents to cloud based repository
- Cloud based data repository: any cloud based data storage can be used to store personal health data – we are currently using Dropbox™ as storage. The contents of the storage are organized by directories and described by Dublin Core Metadata for interoperability (except for HL7 CDA files)

The data can be collected and uploaded to cloud storage based on three data types:

- Observed symptoms: Entered by patients themselves or legal guardians (e.g. observation of chest pain, shortness of breath, fatigue etc.). We have developed a standard medical code browser for SNOMED CT that is used to describe a patient's problem list. We have developed a SNOMED CT browser to provide corresponding SNOMED code for the observed symptoms and measurements.
- Measurement data from portable medical devices or sensors can be inputted using PMHRS to create HL7 CDA files
- EHR data which is collected from healthcare provider. For the non-HL7 CDA data formats, the Dublin core metadata will be used to describe that what the document is about in order to retrieve data faster and organized them as well as keep tracking of the data resources.

The Dublin Core Metadata Initiative, or DCMI, is an open organization supporting innovation in metadata design and best practices across the metadata ecology.

Figure 3. Proposed hybrid PHR architecture

5. CONCLUSIONS

In this study, we surveyed articles related to PHRS from 2008 to 2016. We have identified barriers from 6 different aspects - motivation, usability, ownership, interoperability, privacy and security, and portability that hinder the adoption of PHRS. We also surveyed existing PHRS system architectures and categorized those into 4 different types in the respective to barrier of PHRS. By considering the survey results, we attempted to address the concerns in using PHRS in the proposed PHRS architecture with the following concepts in mind: separating clinical data from the applications for flexibility, embracing standardized medical codes and processes for interoperability, and making the clinical data searchable using any applications that are compliant to the standards. As for the future work:

- automate personal clinical data collection process using personal medical device and Raspberry PI
- build interface for any electronic health record systems that are compliant with the meaningful use up to stage 2
- build secure cloud storage that can be used to store sensitive personal clinical and non-clinical data

REFERENCES

[1] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10),pp. 89-106, Sept. 2010.

[2] H. Lo¨ hr, A.-R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud," Proc. First ACM Int'l Health Informatics Symp. (IHI '10),pp. 220-229, 2010.

[3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), June 2011.

[4] Narayan, M. Gagne´, and R. Safavi-Naini, "Privacy Preserving EHR System Using Attribute-Based Infrastructure," Proc. ACM Cloud Computing Security Workshop (CCSW '10), pp. 47-52, 2010.

[5] "The Health Insurance Portability and Accountability Act,"http://www.cms.hhs.gov/HIPAAGenInfo/01_Overview.asp,
2012.