**❖❖ Scientific
❖❖ Research**

Cloud Computing Based PHR Architecture Using Multi Layers Model

Shinji Kikuchi[1], Shelly Sachdeva[2], Subhash Bhalla[1]

[1]School of Computer Science and Engineering, University of Aizu, Fukushima, Japan; [2]Jaypee Institute of Information Technology, Noida, India.
Email: d8111106@u-aizu.ac.jp, shelly.sachdeva@jiit.ac.in, bhalla@u-aizu.ac.jp

ABSTRACT

There are important requirements for the adoption of innovative practices in the medical area. In this context, Personal Health Records have been proposed and some services have already been launched. However so far, there have been only a few studies in regards to applying Cloud architecture for PHR, despite the occurrence of a large volume of data. In particular, the existing studies tend to remain at applying them partly, instead of a full adoption based on the architectural characteristics of the service models. In this paper, we clarify the result of the general architecture design by applying the Cloud components for supporting healthcare record areas and highlight the required conditions to realize it. Through the proposed considerations the requirement for the new techniques of query processing has been identified as one of the critical factors, that are combined with several items such as managing semantic interoperability, managing service level agreement and secret sharing. Accordingly, we propose the primary work for building the standardized, detailed and more sophisticated architecture.

Keywords: Personal Healthcare Records; Architecture Design; Query Processing; Secret Sharing; SLA

1. Introduction

Within the medical area, the role of IT has drawn a lot of attentions. For example, the Health Information Technology for Economic and Clinical Health (HITECH) Act within the American Recovery and Reinvestment Act set aside billions of dollars in federal funding for health IT, particularly Electronic Health Record (EHR) technology. As hospitals move toward meeting the requirements for the meaningful use of EHR, industry observers expect administrators to look increasingly to mitigate the capital expenses and maintenance costs of traditional storage solutions. Major EHR vendors provide a host of conventional client/server offerings, but more Cloud-based health IT options are becoming available. Based on this situation, Personal Health Record (PHR) has been proposed, and has greatly captured our attentions [1]. In particular, in the industry Google Health [2] and Microsoft HealthVault [3] were launched (However, Google Health was discontinued as of January 2, 2012). Accordingly for example, patients can choose to share information stored in their Microsoft HealthVault accounts with their providers. Then, using Microsoft Amalga, Health Information Exchanges (HIEs) and Regional Health Information Organizations (RHIOs) are able to mobilize healthcare information electronically across organizations in a region or community seamlessly and rapidly bringing together current data from a wide variety of clinics and hospital departments and making it shareable. Thus, applying them can leverage to provide a more complete view of a patient's situation and proactively optimize care.

In general, Personal Health Record is an electronic application through which individuals can access, manage and share their health information, and that of others for whom they are authorized, in a private, secure, and confidential environment [4]. PHR systems are more than just static repositories for patient data; they combine data, knowledge, and software tools, which help patients to become active participants in their own care. However, generally healthcare record systems depend on the social and legal systems and frameworks of individual countries. Therefore, there are few cases where the border between traditional EHRs and PHRs might be ambiguous despite the previous definition [5]. Currently, in spite of these constraints, there are several studies on the architectural features of PHRs as mentioned in the next Section. Although there might still be strong dependencies on and constraints from social and legal systems in individual countries, PHRs will also have the functionality in regards to life log aspect, instead of remaining as a mere

extension of EHRs [6]. Thus, the potential requirements on scalability of PHRs will be higher than the traditional EHRs. Therefore, PHR studies must consider Cloud Computing.

The Cloud Computing providers own the hardware and the hosts managing all of the services to the clients according to their usage needs. Virtualization, on the other hand creates virtual versions of technologies like servers, operating systems, network resources and storage devices. It basically enables a single user to access multiple physical devices. In virtualization, either it's one operating system using multiple computers to evaluate databases, or a single computer controlling several machines. Cloud computing leverages economies of scale to reduce inefficiency and improve performance of IT operations. According to the National Institute of Standards and Technology (NIST), there are five characteristics essential to a Cloud Computing system. These are a broad network access, resource pooling, rapid and elastic provisioning, measured service and an on-demand self-service. In particular, for example L. M. Vaquero, *et al.* discuss the relationship of the entire architecture of Cloud Computing together with the elemental service models such as SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service), in order to clarify their roles [7].

However so far, there have been only a few studies in regard to applying Cloud architecture in PHRs as is mentioned in the following section. Therefore, it is required to identify the entire spectrum of PHR using the facilities of Cloud Computing. We have envisioned PHR as typically a health record which is initiated and maintained by an individual. An ideal PHR would provide a complete and accurate summary of the health and medical history of an individual by gathering data from many sources, including EMRs and EHRs, and making this information accessible to those who have the necessary electronic credentials to view the information. Thus, one PHR is worth nothing. Two PHRs connected to each other are worth something. A network of PHRs is very valuable. The network of PHRs could act as a value multiplier. Without a network the value multiplier is zero. Based on this motivation, we mention the review of our trial on the general architecture design by applying Cloud Components into the healthcare records area, and also highlight the required conditions to realize it. In particular, we briefly evaluate the possibility of the characteristics of Cloud Computing, SaaS, PaaS and IaaS under the healthcare record context. Therefore, the requirements of security and privacy are considered as well. As pointed out, it is difficult to consider the common, ideal and single architecture for PHRs due to the dependencies on the legal systems in individual countries. Therefore, in our consideration, both aspects of EHRs for the healthcare pro-

viders and professionals and that of PHRs for individual common citizens might be contained. Then, the issues on the electronic secret share as an applicable solution for the security requirements will be pointed out under the context of integration with query processing, managing semantic interoperability and service level agreement.

The remainder of this paper is organized as follows. In Section 2, we list the related works. Then, in Section 3, we describe the general aspects of the current dominant architecture of the EHR especially in Japan. In Section 4, we briefly mention our proposal enhancement to the architecture for the healthcare records adopting the Cloud business models. In Section 5 we mention the structural issue on secure query processing. We will touch on the electronic secret share (e.g. [8]) harmonizing with the IaaS as an applicable solution for the security requirements. Finally, in Section 6 we will conclude and talk about the future direction.

2. Related Works

Currently, there are several studies on the architectural features of PHR. For instance, D. Daglish and N. Archer discuss the architecture from the point of view of security and privacy [9]. J. Lahteenmaki, *et al.* consider the interoperability issues of PHR instead of the traditional EHR [10]. Then, R. Fox, J. Cooley and M. Hauswirth discuss the adoption of mashups in this area [11].

Whereas, there have also been a few studies in regard to applying Cloud architecture in PHR. For example, H. Lohr, *et al.* define the notion of the Trusted Virtual Domain based on ordering the issues of security [5]. N. Botts, *et al.* mention the adoption of Cloud Computing in their HealthATM [12]. However, due to the issues of security which the Cloud Computing itself has, the degree of the progress of applying it into a PHR looks not quite up to speed yet. In the work of [12], under the context of considerable issues in Cloud Computing, the scalability is touched on. However there are few concerns about the volume of data in it. Furthermore, clarifying the relationships with the mentioned SaaS, PaaS and IaaS looks like a remaining challengeable issue.

On the other hand, in industry Microsoft has launched a web page [13] where consumers using PHR from Google Health can have their personal health information transferred to a Microsoft Health Vault account. As the demise of Google Health brings into sharper focus the challenges of establishing an online PHR business model, PHRs will see a 33% gain in revenue through 2015 as doctors push patients to use health IT systems [14].The Microsoft Connected Health Framework (CHF) architecture [15] consists of process models, service models and information models. Recently, Microsoft has also adopted the archetype-based approach (initially proposed

by openEHR [16]) for EHRs.

3. Current Major Architecture

Figure 1 shows the "To Be" architecture model considered in general in Japan. Under the Japanese institution, the model consisting of three layers is applied based on the social and actual requirements [17]. And that is totally different from the uniformed approach over countries, which was adopted in NHS of UK [18].

The core part of this architecture is the Regional Healthcare Information Sphere (RHIS) orientated to a decentralized system in the individual regions. Therefore, it might be an urgent and mandatory matter to establish the notion of the RHIS and to define the set of concrete compartments of it under practical constraints. A primary hospital will administrate the integration of related information of the charged region. And inside each RHIS, their interoperability of exchanging the information should be established by their autonomy. Medical service providers in small scale under a RHIS will establish their interoperability with the superior primary hospital in that RHIS by a relatively autonomic approach. As for the national level as the top, the National Healthcare Information Network will be established by integrating all of the RHISs. Accordingly, the standardizing activities in regard to interoperability efforts, such as, ontology will be executed in parallel together with establishing a set of RHIS. By applying the notion of commissioned RHIS, it is predictive that risks in regards to security and privacy might relatively be mitigated. However, it might also invite some constraints in regards to providing the more quality advanced services, which will be based on the extracted facts from the gathered volume data. In Japanese case, the draft plan with respect to deploying PHRs, which are different from traditional EHRs managed by medical service providers, was previously considered under the initiative from the Japanese government. However, spreading PHRs in the practical level had little progress due to several reasons, such as, constraints of the business models and insufficient degree of the spread of digitization in electronic medical records [19].

Under the current blue print in regards to RHIS depicted in **Figure 1**, it is still ambiguous to realize the practical requirements for scalability. Instead, the solutions for applying Service Oriented Architecture (SOA) and interoperability on the semantic level (through archetypes), observed in several efforts such as, openEHR seems to be more prioritized [16]. At present, it supports services such as, "HER" and "Demographics" with means of accessing other key resources such as, terminology. The service layer includes a "virtual HER" for decision support.

Figure 2 depicts the reference architecture for health

and social care specified in Microsoft Connected Health Framework Architecture and Design Blueprint [15]. This is a function wise reference layer model of the Health-Care system and applicable to the PHRs. In [15], there are descriptions of the various applied cases as examples; however we have considered that it seems to remain as a general reference model. Therefore, when we try to apply the particular Cloud business models such as, PaaS and IaaS it is obvious that we need to clarify the more detail components.

4. Enhanced Model Architecture

4.1. Overview

In **Figure 3**, we depict the result of our trial consideration for the ideal architecture. In this figure, we have drawn a RHIS appearing in the previous **Figure 1**. However, it should conceptually be a more generalized healthcare service provider as a business entity.

In the PHR, as huge amount of data will be generated because of measuring the individual's physical daily conditions as their life logs, these data must be maintained due to managing them with the aspect of temporal data. Therefore, both of the following items must be treated as mandatory matters; the first is the architecture orientating to the scalability. The second is to establish the insurance of security and privacy. Furthermore ideally, it might be required to make the data belonging to the individual independent from the management by all of the medical service providers as business entities and to integrate them by shifting them to the individual's responsibility. Accordingly, it is ideally preferable to realize the following two items; the first is to make the management functions on data owned by individuals more virtualized and to exchange them through the functionality such as the service bus flexibly. The second is to deploy all of the applications and services, which are owned by the business entities, on the above service bus as the upper layer. Here, it strongly seems suitable to adopt the architecture where the data management should be implemented as a transparent hub by applying the PaaS model as the lower boundary. As for the service bus, there is already an existing instance implemented by LENUS [20].

There are certain needs to seek data under entries in a time series due to the aspect of temporal data, which PHRs have [21]. Thus, both of the treatments for preparing the growth of data volume and for realizing the usual availability are required at the same time. For example, consider 'ECG results', where one concept corresponds to 10 leads' worth of time-series data, potentially hundreds of samples. Due to these reasons, it might be required to make the configuration around disk facilities more dynamic and flexible, and to regard generic IaaS
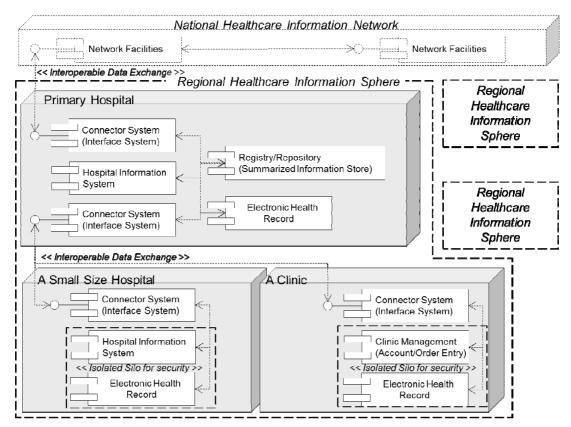
Figure 1. An example of current architecture of Electronic Healthcare Record.
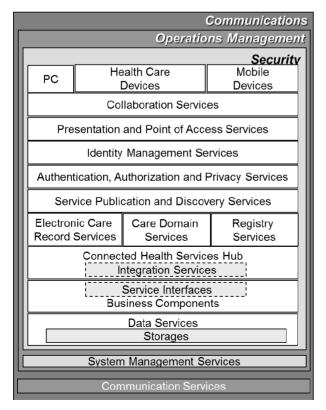

Figure 2. Reference architecture of Microsoft connected Health Framework and Design Blueprint.

services as outsourcers for potential and more practical partners. However, the strict security and privacy must be assured somehow due to the features of treated data. More details will later be mentioned in Section 4.2.

Furthermore, the analysis of clinical trial data for improving the quality of medicine and medical services, and that of daily habits and behaviors of individuals for proactive medical protection are also required. More in detail will be addressed in Section 4.3.

4.2. Data Store

The current status on security and privacy in regards to a PHR is pointed out in [9,22]. A recent study discusses secure electronic medical record sharing mechanism in the Cloud Computing platform [23]. In order to manage the medical privacy data by utilizing a safer approach, applying the encryption inside data stores is one of the ways. However, it is not preferable to depend on management carried out by contracted IaaS service providers fully, even though encrypted data inside data stores is specified. Thus, the ideal data, which are maintained at contracted IaaS providers, is merely the fragments of data, which loses the definition of the internal structure and their semantics.

One of the approaches to realize the above situation is by applying secret sharing. In this approach, several data

will be gathered once, integrated together, further divided in another way and deployed as individual fragments on the distributed nodes. If a piece of divided data is lost, it is impossible to regenerate the original meaningful data even by using all of the remaining fragments of divided data. By applying this secret sharing with combining the distributed storages provided by IaaS service providers, more improved encryption as a safer approach will be realized. However, there are also challenges such as quick decryption in queries (touched in Section 5).

4.3. Mining Functionality

In order to realize the advanced digitized services, the new knowledge based on the facts must be acquired. Therefore, the set of mining processes should be operated under the integrated environment, after executing the processes of anonymity on gathered and maintained data. Furthermore, it is ideally important to make the series of the above set of processes as a seamless in-process including points for decision making as the market approaches. As concrete instances, they correspond to the processes such as evaluation on adverse effectiveness of new drugs [24], and the acquisition of new knowledge in regards to general healthcare services [25]. The Microsoft CHF architecture includes services for knowledge management and decision support. In particular, it is also required to give back an advice to patients, which contains valid and contributable contents such as improved plan for daily life and daily behaviors. In order to achieve these processes responding to patients, the software framework and foundations as mining components and engines must be provided as a service. This should be an extension of SaaS model.

These functionalities should be embedded in the implementations of service provider sides to respond to the flexible demands.

4.4. Components of the Architecture

The significant components of the architecture depicted in **Figure 3** are explained. As one of the major components, "Common Facilities" are defined. In the case of openEHR, the reference architecture incorporates the segregation between a healthcare information such as clinical treatments, diagnoses and demographic information containing identifiable privacy items such as name, age, address and occupation. Therefore, this healthcare information should be stored at different sites from the demographic information. This helps in achieving anonymity as there are no direct clues of identity of patient in the PHR. Instead, demographics data would be provided by other sites and which are expected to be maintained through the national identification numbers or national insurance numbers which should be used as the patient

identifiers. These Common Facilities are modeled as the above generalized providers of demographic information.

Inside of the PaaS provider, there are components named as "Archetype/Semantics/Catalog Manager" and "Query Processing Optimizer". In order to realize more efficient operations with spread data of PHR, the semantic interoperability is required. Therefore, conceptual models such as a set of archetypes should be implemented. "Archetype/Semantics/Catalog Manager" is substantially equivalent with the meta-data manager named "Data Dictionary/Directory" inside of the traditional ANSI/X3/SPARC model. A replica of "Archetype/Semantics/Catalog Manager" could also be deployed at an IaaS provider. In our ideal case, the data stored at an IaaS provider is merely the fragment losing the meaning of original data. However, the common definition part of data which corresponds to the archetypes is not critical for protection of privacy. In order to optimize the query processes, Archetype definitions could be shared with IaaS providers instead of implementing it only on the PaaS provider in isolation. "Query Processing Optimizer" is the function for parsing the query expressions in query languages such as AQL (Archetype Query Language) [26], decomposing the intermediate expression into sub processes, and selecting the most economical execution plan over all. In this case, there are several crucial factors for the evaluation, which are related to not only the generalized statistical approach on the amount of data and constraint rules, but the service level agreements with the IaaS providers as well. The remaining items will be explained at Section 5.3.

"Service Level Agreement (SLA) Manager" maintains all of the agreed operational conditions between the PaaS provider and the set of IaaS providers. Based on the these conditions, "Grid Controller" component and "Secret Sharing" component which can decide the location of data when executing the transactions will carry out their processes. The open issues in respect to SLA will be touched on at Section 5.4. These types of agreements usually cover service availability but not application performance.

The legacy EHR is modeled inside of RHIS. This is defined because the current scenario considering the RHIS is not based on the archetype-based modeling approach. However, in order to realize the more efficient operations with spread data of the PHR, the semantics interoperability realized by applying archetype-based modeling are definitely required. Therefore by combining a translator, the legacy EHR should be packed in a module of data resource for the legacy data. Recently, several efforts and tools have been developed for this purpose at [27-29].

Finally, in **Table 1** we show the comparison between the current major architecture and the enhanced model
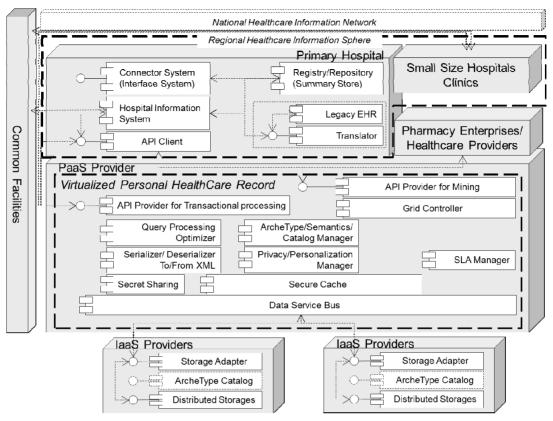
Figure 3. Enhanced model architecture for PHR.

Table 1. Comparison of both architectures.

Features	Current major architecture	Enhanced model architecture
Scalability	Provisioning, sizing with estimation before operation.	Enhancing scalability by adopting IaaS flexibly.
Security and privacy	Depends on current major methods such as 1) Column level encryption. 2) Separated, distributed identifier data. 3) Anonymization.	1) Separated, distributed identifier data. 2) Additionally applying secret sharing.
Cloud based	No particular features because of the traditional approaches.	Considering SaaS, PaaS and IaaS incorporation.
Mining functionality	1) Independent from usual operations. 2) Need to be implemented outside. 3) Less transparency with usual operation.	1) Implemented as an extension of SaaS model. 2) Aiming the seamless data sharing. between operations and analysis.
Semantic interoperability	Not considered.	Included by addition of archetype/semantic/catalog manager.

architecture as our proposal within the several key features.

5. Secure Query Processing

5.1. Overview

Recent research discusses policy approaches to Cloud-based PHR and categorize into four options: Prevent it, Delay it, Attempt to shape it to the needs perceived by the policymakers or Just let it happen [30]. SAP Technology Lab, China is developing a clouds-enabled information appliance, Xbase, built on top of Hadoop, which is the first XML-based information appliance designed specifically for large scale and complex healthcare applications [31]. However, the following matters still require further addressing.

- Security and privacy;
- Complicity of queries processing;
- New issues in secure query processing.

5.2. Security and Privacy

The central goal of PHR platforms such as Microsoft HealthVault, and DossiaIndivo [32] is to let patients use their health information for better self-management via the applications and services built on these platforms. Thirdparty applications such as Livestrong (http://livestrong.com) and TrialX (http://trialx.com) re-use the data within a patient's PHR (with due patient consent and with required measures to protect patient privacy) and provide personalized and useful services. However, the highly regulated nature of health care, particularly the requirements imposed by the Health Insurance Portability and Accountability Act (HIPAA) [33], has created obstacles to the rapid adoption of cloud services in the industry. The mechanisms for security are required for distribution and access of information. The security features such as, support for transport level encryption, protocol to allow transmitting users and protocol to enforce access rules should primarily be considered for the proposed architecture. However the public/ private Cloud are still a point of concern [34]. Therefore, by applying the secret sharing with combining the distributed storages provided by IaaS service providers, more improved encryption as a safer approach will be realized.

5.3. Complicity of Queries Processing

In order toprovide interoperability, PHRs must support the same communications, messaging, and content encoding standards as other health information systems. Microsoft architecture has considered implementing archetype based architecture for achieving interoperability. Thus, all services should be archetype/template awareto gain semantic interoperable gains. The query service based on AQL/archetype path (a-path) has been proposed recently by openEHR. It is portable in comparison to the SQL queries against the physical database.

Health care providers as SaaS have expressed concerns about accessing patient data if that information is stored by a Cloud services provider as PaaS. Querying under such scenario is a major point of concern. The following considerations may be taken into account.

Query evaluation: User run queries should be evaluated based on the privacy policy to make sure they do not violate it. In case of violation, appropriate measures should be taken. For example, controlled query evaluation enforces security policies for confidentiality in information systems [35].

Query modification: They should provide a means

where user queries can be modified. This is important in healthcare environment when user wants to query data from another hospital.

Extended log: A log should include queries that a user ran. This log combined with new queries can be used to evaluate queries in order to prevent privacy policy violations.

Furthermore, due to query data from another primary hospital, we need to take semantic interoperability into our account. As the technology matures further and the healthcare industry embraces semantic interoperability concerns, the chance for a successful health IT transformation with the use of the cloud significantly increase. In order to share and compute with health data at any level of detail, we need a knowledge-based architecture. It is achieved through the addition of archetypes-based services offered on Cloud. Knowledge-based architecture brings new needs, such as:

- New knowledge services-archetypes and reference-sets;
- Other services must be knowledge-aware.

5.4. New Issues in Secure Query Processing

Under the above complicity of queries processing, we need also consider the secure implementation. In this case, there are several encountered issues.

- The first is how to deploy the functionalities in regards to query evaluation, query modification, extended log and the repository for managing the archetypes. As mentioned, the data management should be implemented as a transparent hub by applying the PaaS model. Further, actual storing them will be done by distributed storages managed by commercial IaaS service providers. Therefore, the architecture for deploying the previous three will be crucial.
- The secret sharing with combining the distributed storages will force us to execute decryption. In particular, the quick decryption in queries is definitely required. Therefore, for example, a secure cache which stores the isolated pre-decryption flat data might be a candidate to realize the both requirements. Further, there are some variations of configuration of the secret sharing from the point of view of operations. Anyway, more detail design and selecting a reasonable approach are required.
- Negotiating the terms of the cloud service agreement prove challenging. How to deploy fragment data caused by the secret sharing onto the distributed storages provided by IaaS service provider is also an important issue, in the particular cases, where a SLA contract manages the applicable conditions.

6. Conclusions

Despite of the demise of Google Health which brings

into sharper focus the challenges of establishing an on-line PHR business model, PHRs will see a 33% gain in revenue through 2015 as doctors push patients to use health IT systems [14]. The cloud based PHR virtually organizes the health information in one place, gathers health/medical records from hospitals, doctors and pharmacies, shares information securely with the doctor, health care provider or family member and analyzes and gains their insights from the health records. Without the reference architecture, it will lead to a collection of independent services, which only increases the complexity. Cloud based orientation has an effect on three domains of business operations: infrastructure, applications and data, and business services. For each of these domains, a business case can be made to evaluate which returns different changes in business operations can deliver, in order to be able to set priorities. IaaS is aimed at better sharing and managing of expensive infrastructural utilities. The heterogeneous complexity of servers, storage, security and network equipment is brought back to orderly, standardized services. SaaS aims at the development of systems of cooperating services that can be quickly, costly and commonly adjusted to new organizational requirements. In the PaaS, the new or modified applications and infrastructure are positioned for the support of business operations aimed at the exchange of services with the outside world.

Thus, this paper briefly discusses how should the regional and national governments formulate their Cloud based IT strategy so as to facilitate communication within the government, between the government and its citizens, and between the government and businesses. To fully exploit the potential benefits of virtualization in healthcare, IT teams need to seamlessly integrate, automate, and standardize infrastructure operations and provisioning activities across server, storage, and network resources. As the future works, we need to develop the suitable solutions for the issues pointed out in Section 5.4.

REFERENCES

[1] C. Ogbuji, K. Gomadam and C. Petrie, "Web Technology and Architecture for Personal Health Records," *IEEE Internet Computing*, Vol. 15, No. 4, 2011, pp. 10-13. doi:10.1109/MIC.2011.99

[2] Google, "About Google Health." http://www.google.com/intl/en-US/health/about/index.html

[3] Microsoft Health Vault. http://www.healthvault.com/

[4] 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 No. 2, 2006, pp. 121-126.

doi:10.1197/jamia.M2025

[5] H. Löhr, A. R. Sadeghi and M. Winandy, "Securing the e-Health Cloud," *Proceedings of the* 1*st ACM International Health Informatics Symposium IHI'*10, Arlington, 11-12 November, 2010, pp. 220-229. doi:10.1145/1882992.1883024

[6] F. Daniel, F. Casati, P. Silveira, M. Verga and M. Nalin, "Beyond Health Tracking: A Personal Health and Lifestyle Platform," *IEEE Internet Computing*, Vol. 15, No. 4, 2011, pp. 14-22. doi:10.1109/MIC.2011.53

[7] L. M. Vaquero, L. Rodero-Merino, J. Caceres and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition," *Newsletter*, *ACM SIGCOMM Computer Communication Review Archive*, Vol. 39, No. 1, 2009, pp. 50-55. doi:10.1145/1496091.1496100

[8] R. Brinkman, B. Schoenmakers, J. Doumen and W. Jonker, "Experiments with Queries over Encrypted Data Using Secret Sharing," *Proceedings of* 2*nd VLDB Workshop on Secure Data Management* (*SDM'*05), Trondheim, 2-3 September 2005, pp. 33-46. doi:10.1007/11552338_3

[9] D. Daglish and N. Archer, "Electronic Personal Health Record Systems: A Brief Review of Privacy, Security, and Architectural Issues," 2009 *IEEE Proceedings of* 2009 *World Congress on Privacy*, *Security*, *Trust and the Management of e-Business*, Saint John, 25-27 August 2009, pp. 110-120. doi:10.1109/CONGRESS.2009.14

[10] J. Lahteenmaki, J. Leppanen and H. Kaijanranta, "Interoperability of Personal Health Records," *Proceedings of Engineering in Medicine and Biology Society*, *Annual International Conference of the IEEE*, Minneapolis, 3-6 September 2009, pp. 1726-1729. doi:10.1109/IEMBS.2009.5333559

[11] R. Fox, J. Cooley and M. Hauswirth, "Creating a Virtual Personal Health Record Using Mashups," *IEEE Internet Computing*, Vol. 15, No. 4, 2011, pp. 23-30. doi:10.1109/MIC.2011.52

[12] N. Botts, B. Thoms, A. Noamani and T. A. Horan, "Cloud Computing Architectures for the Underserved: Public Health Cyberinfrastructures through a Network of Health ATMs," *IEEE Proceedings of* 43*rd Hawaii International Conference on System Sciences*, Honolulu, 5-8 January 2010, pp. 1-10. doi:10.1109/HICSS.2010.107

[13] Microsoft Health Vault, "Welcome, Google Health Users." http://www.microsoft.com/en-us/healthvault/google-health.aspx?WT.mc_id=M11071406&WT.ad=text::GHConvertPR::MSPress::HvGH::1406

[14] N. Lewis, "Google Health Dies, but PHR Market Still Growing," *Information Week*, 2011. http://www.informationweek.com/news/healthcare/EMR/231000876

[15] MicroSoft, "Connected Health Framework Architecture and Design Blueprint," 2009. http://www.microsoft.com/health/ww/ict/Pages/Connected-Health-Framework.aspx

[16] openEHR, 2007. http://www.openehr.org/home.html

[17] Japan Association for Medical Informatics, "Health Informatics: Health Information Systems," Shinohara Shup-

pan Shinsha, 2009. (In Japanese)

[18] OASIS Open and BT, "Case Study: UK National Health Service NPfIT Uses ebXML Messaging," 2004. http://xml.coverpages.org/ebXML-NHS-CaseStudy20041 206.pdf

[19] Minister of Economy, Trade and Industry of Japan, "Summary report on PHR in Japan (in Japanese)," 2008. http://www.meti.go.jp/policy/mono_info_service/service/ downloadfiles/phr_houkoku_gaiyou.pdf

[20] D. Krechel and M. Hartbauer, "The LENUS Master Patient Index: Combining Hospital Content Management with a Healthcare Service Bus," *Proceedings of* 21*st IEEE International Symposium on Computer-Based Medical Systems. CBMS*'08, Jyväskylä, 17-19 June 2008, pp. 170-172. doi:10.1109/CBMS.2008.107

[21] T. D. Wang, K. Wongsuphasawat and C. Plaisant, "Visual Information Seeking in Multiple Electronic Health Records: Design Recommendations and a Process Model," *Proceedings of the* 1*st ACM International Health Informatics Symposium IHI*'10, Arlington, 11-12 November 2010, pp. 46-55. doi:10.1145/1882992.1883001

[22] L. Martino and S. Ahuja, "Privacy Policies of Personal Health Records: An Evaluation of Their Effectiveness in Protecting Patient Information," *Proceedings of the* 1*st ACM International Health Informatics Symposium IHI* '10, Arlington, 11-12 November 2010, pp. 191-200. doi:10.1145/1882992.1883020

[23] Z. R. Li, E. C. Chang, K. H. Huang and F. Lai, "A Secure Electronic Medical Record Sharing Mechanism in the Cloud Computing Platform," *Proceedings of* 2011 *IEEE* 15*th International Symposium on Consumer Electronics* (*ISCE*), Singapore, 14-17 June 2011, pp. 98-103. doi:10.1109/ISCE.2011.5973792

[24] R. Harpaz, K. Haerian, H. S. Chase and C. Friedman, "Mining Electronic Health Records for Adverse Drug Effects Using Regression Based Methods," *Proceedings of the* 1*st ACM International Health Informatics Symposium IHI*'10, Arlington, 11-12 November 2010, pp. 100-107. doi:10.1145/1882992.1883008

[25] G. Luo, C. Tang and S. B. Thomas, "Intelligent Personal Health Record: Experience and Open Issues," *Proceedings of the* 1*st ACM International Health Informatics Symposium IHI* '10, Arlington, 11-12 November 2010, pp. 326-335. doi:10.1145/1882992.1883039

[26] C. Ma, H. Frankel and T. Beale, "openEHR, Archetype Query Language Description," 2009. http://www.openehr.org/wiki/display/spec/Archetype+Query+Language+Description

[27] J. A. Maldonado, D. Moner, D. Tomás, C. Angulo, M. Robles and J. T. Fernández, "Framework for Clinical Data Standardization Based on Archetypes," *Studies in Health Technology and Informatics*, Vol. 129, 2007, pp. 454-458.

[28] C. Rinner, T. Wrba and G. Duftschmid, "Publishing Relational Medical Data as prEN 13606 Archetype Compliant EHR Extracts Using XML Technologies," 2007. http://www.meduniwien.ac.at/msi/mias/papers/Duftschmi d2007b.pdf

[29] D. Moner, J. A. Maldonado, D. Bosca, J. T. Fernandez, C. Angulo, P. Crespo, P. J. Vivancos and M. Robles, "Archetype-Based Semantic Integration and Standardization of Clinical Data," *Proceedings of the* 28*th IEEE EMBS Annual International Conference*, New York, 30 August-3 September 2006.

[30] W. Rishel, "The Cloud Based Personal Health Record," Industry Research ID No. G00158181, Gartner, 13 June 2008, pp. 1-9.

[31] W. S. Li, J. Yan, Y. Yan and J. Zhang, "Xbase: Cloud-Enabled Information Appliance for Healthcare," *Proceedings of the* 13*th International Conference on Extending Database Technology (EDBT*'10*)*, Lausanne, 22-26 March 2010, pp. 675-680. doi:10.1145/1739041.1739125

[32] Dossia Indivo, "INDIVO^{TM}: The Personally Controlled Health Record." http://indivohealth.org

[33] US Department of Health & Human Services, "Understanding Health Information Privacy." http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

[34] D. Agrawal, A. El Abbadi and S. Wang, "Secure Data Management in the Cloud," *Proceedings of* 7*th International Workshop on Databases in Networked Information Systems* (*DNIS* 2011), Aizu-Wakamatsu, 12-14 December 2011, pp. 1-15. doi:10.1007/978-3-642-25731-5_1

[35] J. Biskup and P. A. Bonatti, "Controlled Query Evaluation for Known Policies by Combining Lying and Refusal," *Annals of Mathematics and Artificial Intelligence*, Vol. 40, No. 1-2, 2004, pp. 37-62. doi:10.1023/A:1026106029043