MEDINFO 2017: Precision Healthcare through Informatics
A.V. Gundlapalli et al. (Eds.)

doi:10.3233/978-1-61499-830-3-35

Electronic Health Records in the Cloud: Improving Primary Health Care Delivery in South Africa

Liezel Cilliers[a], Graham Wright[b]

[a] Department of Information Systems, University of Fort Hare, East London, Eastern Cape, South Africa,
[b]Department of Health Sciences, University of Fort Hare, East London, Eastern Cape, South Africa

Abstract

In South Africa, the recording of health data is done manually in a paper-based file, while attempts to digitize healthcare records have had limited success. In many countries, Electronic Health Records (EHRs) has developed in silos, with little or no integration between different operational systems. Literature has provided evidence that the cloud can be used to 'leapfrog' some of these implementation issues, but the adoption of this technology in the public health care sector has been very limited. This paper aims to identify the major reasons why the cloud has not been used to implement EHRs for the South African public health care system, and to provide recommendations of how to overcome these challenges. From the literature, it is clear that there are technology, environmental and organisational challenges affecting the implementation of EHRs in the cloud. Four recommendations are provided that can be used by the National Department of Health to implement EHRs making use of the cloud.

Keywords:

Electronic health records; cloud computing; primary health care

Introduction

The primary health care system in South Africa is facing many challenges. These difficulties include the high disease burden consisting of infectious and non-communicable diseases, persisting social disparities, and a lack of qualified health staff. South Africa's population is currently estimated in approximately 54 million people, while 54% of this population lives below the poverty line [1]. It has been reported that in South Africa 84% of the population cannot afford a medical aid, and thus making use of the public health care sector, which only employs 20% of the health care workers in the country [2].

The shortage of primary health care facilities is most acute in the rural areas of the country. Patients living in these areas often travel far distances at considerable cost to access health care services [3]. When the primary care facility cannot treat the patient, they are referred to the next tier in the health care system, which is the secondary level district hospital, or the last tier, that provides tertiary services, and these are often located far away in the city. Thus, patients can have many health care providers throughout the public health care system, all of which will have their own health care records for the particular patient. If the file is misplaced at the health care facility, a new file must be opened and all the medical history before the event is lost. This means that patients often have multiple files at a single facility. To exacerbate the situation, if the patient move to another region or province, their health record will remain behind, and their health care record will have to be started anew [4].

The most common method to record health care data in South Africa is a manual, paper-based health records. The National Department of Health (NDoH) has made attempts in the past to implement an electronic health record system to improve the continuity of care, but these efforts were fragmented at best resulting in interoperability issues between the various systems being used [4]. While the cloud can overcome the problem of interoperability as one system can be made available to every health care facility in South Africa, the adoption of the cloud in the public health care sector in the country has been slow. Some of the reasons provided for the slow adoption of the cloud are security concerns, trust of the cloud, and compliance to legislation [5]. The aim of this paper is two-fold: First, the challenges why the cloud has not been used to implement EHRs in South Africa will be investigated, and second, recommendations to overcome these obstacles will be provided. The next section will discuss the definition and use of electronic health records in the South African public health care system.

Electronic Health Records

According to the Health Information and Management System Society [6], although the terms EHRs and electronic medical record (EMR) are often used interchangeably, they actually refer to separate concepts. An EMR is a local, stand-alone health information system that allows for the storage, retrieval and modification of health records. The EMR refers to the legal patient record that is created in the health care environment, by the health care worker, and becomes the data source for the EHR.

The EHR is an electronic version of the patient's medical history, which includes clinical data and history, progress notes, medications, vital signs, past medical history, immunisations, laboratory data, radiology reports, and administrative data. The EHR can be shared among health care providers at the same hospital and across different health care settings through an information system that is connected via a network, e.g. the cloud [3, 5]. However, many patients have privacy concerns when their medical data is stored in an EHR.

Privacy in the context of EHRs means that the patient must retain control of their own information even if it is 'owned' by another party, such as the hospital. This control extends to whom is authorized to access a copy of the data, e.g. where billing records are shared with the medical aid company, or different health care workers are authorized to view the EHR [7]. The EHR must be delivered in an environment in which patients have absolute confidence that their privacy will be protected and that the confidentiality, integrity and availability of the information stored in EHR will be assured [3]. The next section will discuss cloud computing in the healthcare sector.

Cloud Computing

Cloud computing has the potential to make health care more efficient and effective. Storage of medical data, processing capabilities of the EHRs, and bandwidth necessary to share the records are centralised to become more efficient. However, while the cloud has been adopted in many industries, the health care sector has been slow to make use of cloud-based solutions [5, 8].

The cloud makes use of internet connectivity and a standard web browser to allow the health care worker to access the EHR. An advantage of the cloud is that the health care organisation do not have to develop or maintain the hardware and software infrastructure necessary for the ERHs, but simply make use of the cloud services and deployment models that best suit their specific operational and technical needs [5].

There are three service models that are applicable to the cloud in the health care sector. The first is Infrastructure as a Service (IaaS) that allows health care workers to provision processing, storage, network, and other resources in which they can deploy and run arbitrary software, such as operating systems and EHRs applications. This means that the health care organisation does not have to manage their own infrastructure and can add computing processing power and storage capacity as the need arise. The main benefit of IaaS is the fast deployment of applications and the improved agility of information technology services within the organisation. However, the NDoH do not have their own EHRs application in place at present. Therefore, this option does not seem appropriate. The second service model is the Platform as a Service (PaaS) that allows for the quick and efficient development of health applications that can be hosted in the cloud. This environment allows the NDoH to build applications with no capital expenditure on infrastructure, as the service provider is responsible for the maintenance and control of the underlying cloud infrastructure. The NDoH could use this model to build their own EHRs, but with the lack of information technology skills in the public health care sector in South Africa, this solution does not seem viable. Third, service providers make use of a Software as a Service (SaaS) model to provide access to applications and software remotely through a web-based service. The cost of accessing these services is typically less than paying for licensed applications, as the health care organisation only pay for the actual time they use the application, and there are no hardware layout costs. The service provider is also responsible for the installation, set-up and maintenance of the services they provide. In this model, the service provider would provide the application for the EHRs, and the NDoH would pay for the usage thereof [9; 10]. This option would also overcome the problem of integration between the various health care facilities, as a single program will serve the South African public health care system.

There are four cloud deployment models: private cloud, community cloud, public cloud, and hybrid cloud. The private cloud is hosted and operated by one organisation, while the community cloud allows several organisations, normally with a common goal to share the infrastructure. The public cloud is owned by an organisation that sells cloud services to the general public or a large industry group. The last deployment model, the hybrid cloud, is a composition of two or more clouds that remain unique entities but are bound together by proprietary technology [10]. The private cloud could be used by one organisation, such as a medical aid company, to provide EHRs to their clients, but this system would not be integrable with other systems outside the company's sphere. A company such as Google that provides EHR services to the public would make use of a public cloud, but there are privacy and security concerns with such a deployment model. The model that is best suited to EHRs, therefore, seem to be a community cloud, as health care providers share a common goal – to provide more efficient and effective access to the medical data of the patient [9, 10].

The benefits of cloud computing to provide EHRs to the public health care service in South Africa can be derived from the discussion above as well as the following [11]:

1. Reduced cost to the NDoH, as they do not have to maintain the information technology infrastructure.
2. The cloud is available on demand to the health care worker and can be accessed from any location.
3. The resource pooling of physical and virtual resources allows for the most efficient use of the technology.
4. The cloud provides flexibility to the NDoH, as it can be easily scaled according to the need and demand of the health care facility.
5. The cloud provides usage metrics that can help the NDoH in the decision-making process for future technology usage and planning. These metrics can also contribute to the sustainability of the EHRs that is provided.

Electronic Health Records in South Africa

HealthID

Discovery Medical Aid is providing an EHR to their clients called Health ID. This EHR is the first of its kind in South Africa according to Discovery. The purpose of HealthID is to collate the medical data and details of all hospital visits, including scripts for medicines, blood tests and health indicators. The patient must provide written consent for each of their health care workers they visit to access their HealthID in order to protect their privacy. The consent can be provided before the appointment or during the visit by accessing the patient's Health ID profile on the Discovery website [12].

The purpose of Health ID is to reduce the administrative burden on the health care worker, as they have access to the full medical history of the patient regardless of where their previous visits took place, as well as the health benefits of the patient. The real-time access allows the health care worker to apply and receive approval for chronic medication and to identify what medication the patient is currently taking, which is especially useful for elderly patients that may not be able to remember [12].

Google Health

This product was available in South Africa through the Google platform from 2008-2012. Google Health provided the patient with an opportunity to manage their own health information, although the EHR could not be shared with the health care worker. Unfortunately, Google Health was not adopted by the general public and achieved only limited use; hence, it was discontinued in 2012. While the system quality of Google Health was found to be appropriate, the system was perceived to be high risk resulting in low trust among users. The lack of awareness among users about the benefits of EHRs contributed to the lack of trust, as well as the failure of health care workers to recommend the product as a useful tool to collect health information. The functionality of Google Health was also limited. The user could not make the application available to their health care provider, but only use it to manage their own health information. Klein suggested that patients were not ready to manage their own health data in 2008, which contributed to the lack of adoption among users [13].

Nompilo service

Vodacom in partnership with local Non-Governmental Organizations and the NDoh launched an application which provided end-to-end monitoring and evaluation for local

community workers in 2009. When these workers visit the patients in the community, they can upload patient information directly to the system making use of their smartphones. Each patient is assigned a unique 2D barcode that can be used to identify them on the system. Nompilo then shows the health care worker what information needs to be collected from that particular patient. Typical information collected include personal, administrative, and physiological data to support the treatment plan. Current and historical patient information can also be viewed remotely, in real time, by the health care worker [14].

Electronic health record systems in the public health care sector

The South African NDoH has also started to implement EHR systems in their public health care sector. Currently, 5 out of the 9 provinces in South Africa have some form of EHR system operational in public hospitals. In the KwaZulu-Natal province, some hospitals use the Medicom or Meditech EHR system, while in the Western Cape province a few hospitals use the Unicare or Clinicom EHR systems. Hospitals in the Limpopo province also use the Unicare or Medicom EHR systems [15]. The implementation of different EHR systems from various vendors presents a challenge, as these systems are built with different underlying database architectures; and therefore, often fail to communicate and share information amongst each other. Also, while these systems have been implemented in some areas, the majority of the public health centres in South Africa still make use of a paper-based filing system [16].

Methods

The research was exploratory in nature, and reviewed literature from previous studies, e.g. articles published in academic journals, books (both print and electronic formats), conference proceedings and websites relative to this study. Electronic databases such as ACM Digital Library, Sage Online Journals, Science Direct, Springer Link and Sabinet Reference were used to find the literature. Research keywords such as 'electronic health record', 'electronic medical record', 'cloud' and 'primary health care' were used as search terms. The reference lists within articles previously identified were also examined to yield additional literature. Inductive reasoning was applied to analyze the literature making use of a thematic content approach. The results of the analysis are discussed in the next section.

Discussion

Duhaime [17] provided the following list of generic barriers that must be considered when cloud computing is implemented in any organisation (Figure 1). These barriers are discussed in the context of EHRs below.

Figure 1 - Generic barriers to the implementation of cloud computing (adapted from Mathew, 2012 [18])

Scale, Cost and Reliability

Performance concerns about the cloud are often based on the scale, availability and the dispersal of the cloud [18]. The technology needs to be reliable and accessible to be useful to the health care worker. In Africa, the primary barriers to the implementation of the cloud include unreliable electricity supply, poor internet connectivity, and limited bandwidth. internet penetration in Africa is the lowest of all the developing world regions, with only 0.3% fixed broadband penetration on the continent, and internet penetration at 16.3% [19]. As an internet connection is needed to access the information in the cloud, these factors will influence the reliability of the EHRs. There are several different factors that will determine the cost of the technology, especially if SaaS service model is used. These include the amount of storage required, network services, scheduling, service level agreements, optimal location of data centres and software components, efficient SQL query processing, architecture and process improvement.

Lock In and Agility

One of the advantages of the cloud is the agility that it provides in regards to capacity, storage and demand. When the NDoH decides to make use of one vendor, they become 'locked-in', as they are then obliged to deal only with that company and their products. If there is a need to migrate away from that vendor, then a significant cost will be incurred. At the present moment, the EHR systems that are used within and across provinces are not integratable [16]. The patient data in these legacy systems will have to be imported into the new EHRs to ensure continuity of care. This may be a problem as the maturity of the technology in South Africa is still low, which means that the industry is not regulated and standardisation between products are non-existent [3].

Change Management

Cloud computing is a new technology that is changing the traditional way of managing health care information in the public health sector. The lack of knowledge about the cloud is one of the reasons the NDoH is reluctant to migrate to the cloud because health care staff and patients are not aware of the cloud's purpose [20]. Due to this lack of understanding, staff may fear that they will become redundant and patients may have misgivings about the safety and privacy of their information and resist the use of the new technology [4].

The failed Google Health application was a prime example of how the relationship between knowledge of the cloud and trust in the cloud is essential for the adoption of the technology. This is because knowledge of the technology is likely to enhance the levels of trust of the user, ensuring it's continued used (Google). Therefore, the NDoH must conduct a needs analysis of their employees' and patients' knowledge of cloud computing before the technology is implemented to manage patient records [10].

Lack of Control

EHRs have to manage sensitive patient information. Comninos [21] found that one of the main reasons why patients and healthcare workers are reluctant to make use of the cloud is concerns about third-party cloud providers that must store or process this sensitive information. Also, connectivity issues are also a concern, as the health care worker can only access information if they are connected to the internet. The lack of

transparency in the cloud is contributing to the control concerns of EHRs. The user is expected to upload their health care information without any knowledge regarding the security measures or controls in place in the cloud. Often, the user does not even know where the information is located, making litigation difficult is something should go wrong [20]

Security

EHRs store and process large databases of sensitive patient information. Many patients have expressed privacy and security concerns if this data is transferred to third party providers of cloud services as the cloud is seen as inherently not secure [20]. The main reason for this perception is that the security in the cloud is intangible and less visible, which creates a concern whether information is stored securely. Security concerns include the altering or loss of sensitive data in the cloud and the unauthorised use of the data by cloud providers [18].

Discussion

In the previous section, the generic barriers for the utilization of the cloud to provide sustainable EHRs services in the public health care service of South Africa were discussed. In summary, the following critical areas were identified:

- Technology: Vendor lock-in; agility and maturity of products available; standardization, reliability and availability of technology; cost of making use of the cloud;
- Organization: Change management including trust; adoption and awareness of the cloud; and
- Environment: Security and privacy concerns.

The following are recommendations that were developed to overcome these critical areas and improve the implementation of EHRs in the cloud. The first recommendation is to provide education to improve the level of awareness about and trust in the cloud, and the benefits it can provide to EHRs. One of the reasons why Google Health failed was because it did not engage with the users showing why EHRs was beneficial to manage their health care, and how cloud computing could help them to manage their EHR. The recommendation is thus twofold as both health care workers and patients need to be educated about the advantages and potential risks of making use of the cloud. With this knowledge gain, it should increase user acceptance and utilization of the technology.

The second recommendation is for the government to provide best practices for both EHRs and cloud computing within a legislative framework. EHRs are already included in the E-Health Strategy for South Africa, but the National Department of Health must also provide a national integrated plan for the implementation of a national EHR system. Best practices, such as to how any service can be implemented making use of cloud computing will also address the problem of vendor lock-in and legacy systems that are not integrable with the national system. Legislation and policies need to be put in place to ensure compliance of the technology with international standards.

The third recommendation is to improve the transparency of the cloud to address the privacy and security concerns. Legislation that provides a proper legal framework, such as the Protection of Personal Information Act, will guide the user, health care worker and cloud provider as to what their rights and responsibilities are. This improves the control on the part of the user and health care workers.

Security controls in place, to protect data, should be provided by third-party cloud providers to assure users that their data is securely stored. Security controls will further improve the transparency of the cloud and provide peace of mind to the patient that the privacy of their sensitive information will be protected. The recommended security requirements include certification, where developers open their cloud applications to security specialists that provide certification for security. Certification will certainly improve the trust of the user in the cloud-based EHRs [22].

- Identification and Authentication: all accounts should incorporate usernames and passwords to verify the user on the cloud, and provide an audit trail of access to that specific EHR;
- Authorization: The challenge is to provide the right information to the right person, while limiting the access privileges of the user. Patients should be able to grant privileges to health care workers, while the functionality of the EHR should be restrictive to who can add or modify information. Patients may not realize why it is important not to change test or laboratory scores. Each user will have to be allocated manually with security clearance to ensure limitation of access to different files;
- Integrity and Confidentiality: encryption techniques should be used to protect sensitive data of the patient;
- Non-repudiation: health care workers and patients must have access to the data at all times for EHRs to be useful. Techniques including digital signatures, timestamps and confirmation receipt services can be deployed to achieve non-repudiation; and
- Availability: It means that the data will be available, accessible and obtainable at all times on the health cloud, while time-outs must be used to restrict access of unauthorized persons if the user forgets to log out of the application.

The fourth recommendation is to address technology problems that may affect the cloud specifically. Cloud computing is still a relatively new technology with limited use in the health sector. Specific technology factors that must be considered include the reliability, cost and availability of the technology. These are important because access to health data must be reliable, if the EHRs is to be of any use. The total cost of migrating to the cloud will decrease, as more deployment options become available. The cost of bandwidth, which is very expensive and limited in South Africa, must also be decreased to make this a viable technology. In developing countries, especially where IT infrastructure is poorly developed, cloud computing makes use of existing internet connections without requiring more infrastructure or financial investments.

Conclusion

This paper provides an overview of the current use of EHRs in South Africa. This includes systems available to the individual patient and the health care worker to manage medical data, and illustrates that EHRs are slowly making inroads in the health care sector. Reasons why the cloud has not been used to provide EHRs in the public health sector of South Africa were divided into the organizational, environmental and technology categories. Four recommendations were provided to how to overcome these challenges that can be used by the NDoH to implement cloud-based EHRs.

Future work would include testing these recommendations making use of an expert review to refine them. It would be useful to investigate the extent of EHRs implementation in the public health care sector and compare these results with the private health care sector. An examination of the adoption of

HealthID among patients belonging to the Discovery medical aid could also provide valuable insight.

Acknowledgements

This research project was jointly funded by the South African Medical Research Council (SAMRC) and Forte, the Swedish Research Council for Welfare, Working Life and Welfare.

References

[1] Statistics South Africa, Mid-year Population estimates (2014). Available at: www.statssa.gov.za/publications/.../P03022014.pdf (accessed 1 November 2016).

[2] BM. Mayosi and SR. Benatar, Health and health care in South Africa--20 years after Mandela, *The New England Journal of Medicine* **371**(14) (2014), 1344–53.

[3] M. Katurura, and L. Cilliers, The extent to which the POPI Act makes provision for patient privacy in mobile personal health record systems, In the proceedings of *IST-Africa*, Durban, 3-5 May 2016, South Africa.

[4] D. O'Mahoney, G. Wright, and L. Cilliers, Electronic health information systems for primary care in South Africa: a review of current operational systems. In the proceedings of *Information Communication Technology and Society Conference*, Umhlanga, 1-3 May 2017, South Africa.

[5] J. Puustjarvi, and L. Puustjarvi, The Opportunities of Exploiting Cloud Computing in Telemedicine: A Developing Country Perspective, In the proceedings of *IST-Africa*, Tanzania, 1-3 May 2012, Tanzania.

[6] HIMSS, Available at: http://www.himss.org/ASP/index.asp. (accessed 10 November 2016).

[7] S. Avancha, A. Baxi and D. Kotz, Privacy in mobile technology for personal healthcare, *ACM Computing Surveys (CSUR)* **45**(1) (2012), 3.

[8] D. Chappel, A Short Introduction to Cloud Computing: An Enterprise-OrientedView. Available at: http://digitalebookden.com/a-short-introduction-to-cloud-platforms.html (accessed 10 November 2016)

[9] S. Subashini, and V. Kavitha, A survey on security issues in service delivery models of cloud computing. J*ournal of Network and Computer Applications* **34**(1) (2012), 1-11.

[10] B. Baize, In cloud we trust. *Cloud computing* **16** (2011), 21-30.

[11] G. Murjithi, and J. Kotze, Cloud computing in higher education: implications for South African public universities and FET colleges. *14th annual conference on World Wide Web applications*, Durban, 2012, 4-24.

[12] Discovery, Discovery Health launches HealthID, 2012.

[13] T. Spil, and R. Klein, Personal Health Records Success; Why Google Health failed and what doesthat mean for Microsoft HealthVault? In the proceeding of the *47th Hawaii International Conference on System Science,* Hawaii 2012.

[14] Mezzanine, Vodacom works with the SA Ministry of Health and local NGOs to provide better healthcare, 2014.

[15] J.E. Ataguba, and D. McIntyre, Paying for and receiving benefits from health services in South Africa: Is the health system equitable? *Health Policy and Planning* **27**(SUPPL.1) (2012), 35–45.

[16] D. O'Mahony, G. Wright, P. Yogeswaran, and F. Govere, Knowledge and attitudes of nurses in community health centres about electronic medical records. *Curationis* **37**(1) (2015) Art.#1150, 6 pages.

[17] D. Duhaime, The Pros and Cons of Cloud Computing. In the Spotlight, 2011.

[18] S. Mathew, Implementation of cloud computing in education - a revolution. *International Journal of Computer Theory and Engineering* **4**(3) (2012), 473-476.

[19] M. Mars, Telemedicine and advances in urban and rural healthcare delivery in Africa. *Progress in cardiovascular diseases* **56**(3) (2013), 326-335.

[20] F. Koch, M. Assuncao, and M, Netto, *A cost analysis of cloud computing for education.* Berlin: Springer, 2012.

[21] A. Comninos, Southern African Internet Governance Forum Issue Papers. Johannesburg: SANGONeT for the Soutern Afric an Internet Governance Forum, 2011.

[22] S. Ramgovind, and M. Eloff, The management of security in cloud computing. *Information Security for South Africa (ISSA),* Johannesburg: ISSA, 2010, 1-10.

Address for correspondence

Corresponding author: Liezel Cilliers.
Email: lcilliers@ufh.ac.za or
Phone: +027 43 7047067.