E-HEALTH DRIVERS AND BARRIERS FOR CLOUD COMPUTING ADOPTION

Marco Nalin, Ilaria Baroni and Alberto Sanna
Fondazione Centro San Raffaele del Monte Tabor, via Olgettina 60, Milan, Italy

Keywords: TClouds, Cloud computing, Electronic health record, EHR, eHealth, Privacy, Security.

Abstract: Cloud Computing is rapidly changing, or at least reorganizing, the IT domain. Several sectors are already benefitting from this change, others are slower in the adoption. Healthcare sector, and eHealth in particular, could take important advantage from Cloud Computing, but there are limitations that still need to be overcome for a proper adoption. This paper explores the main drivers that could lead eHealth toward Clouds and the main risks and recommendations that should be taken into account.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

1 INTRODUCTION

There is a lot of discussion around Cloud Computing and whether it is just a marketing buzz, a new word for describing already existing technologies or something really innovative that will change the IT service models. The definition of Cloud Computing itself is already quite controversial, not only are there hundreds (or even thousands) of versions around the Net, but there are also several articles and websites trying to summarize a unique definition. Being free to choose any of them, we opt for the generic definition provided by IBM (Amrhein and Quint, 2009): "*cloud computing is an all-inclusive solution in which all computing resources (hardware, software, networking, storage, and so on) are provided rapidly to users as demand dictates*".

As expressed in Berkeley view on Cloud Computing (Armbrust, 2009), there are some common characteristics in the definitions: 1) the *infinite availability of resources*, accessible on demand at least in the users' perception, 2) the elimination of *big initial investments* from the users, and 3) the *pay-per-use* business model.

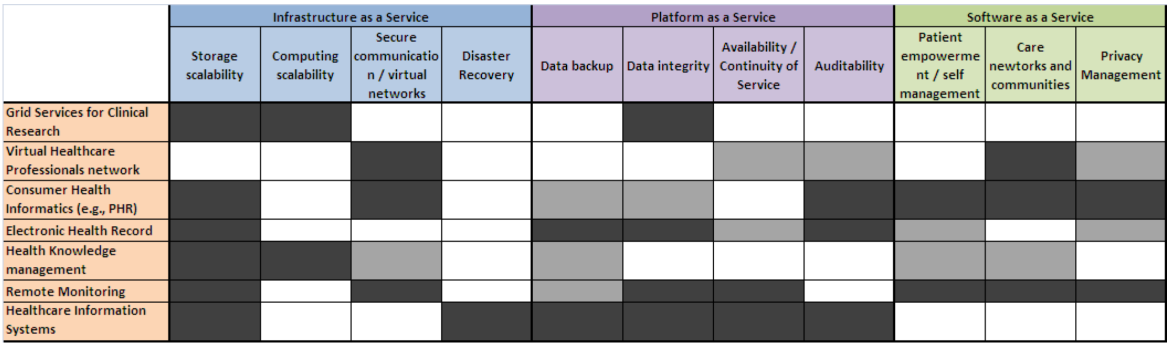
Also the term "eHealth" is very generic and it encompasses a set of different application domains. The macro areas that are nowadays referred to as "eHealth" regards technologies that makes the a) patient's life, b) the doctor's life and c) the medical information exchange and processing easier. These areas are:

- **Grid Services for Clinical Research:** in clinical practice, medical research and personalized healthcare, there's a growing demand for the integration and exploitation of heterogeneous biomedical information. Grid technologies are taking place to federate different data sources, providing access and query functionalities to distributed information in a unified and integrated way. Moreover, they are able to offer ? without interruption computing resources.
- **Virtual Healthcare Professionals Network:** many times, healthcare professionals need to cooperate or exchange information about patients and clinical practice. These networks allow professional teams to collaborate and share data or opinions, about patients or other specific arguments, through digital facilities.
- **Consumer Health Informatics** (e.g., PHR)**:** this domain includes more or less all the electronic resources that can be used not only by patients but also by healthy individuals, for topics on medicine or healthcare.

A clear example is the PHR (Personal Health Record), defined by Markle Foundation definition as "*an Internet-based set of tools that allows people to access and coordinate their lifelong health information and make appropriate parts of it available to those who need it"* (Markle Foundation, 2003, p. 14). Two examples of PHR are Google Health and Microsoft HealthVault.

- **Electronic Health Record:** the EHR is the personal record created by hospitals, clinics or other

Nalin M., Baroni I. and Sanna A..
E-HEALTH DRIVERS AND BARRIERS FOR CLOUD COMPUTING ADOPTION.
DOI: 10.5220/0003379703850390
In *Proceedings of the 1st International Conference on Cloud Computing and Services Science* (CLOSER-2011), pages 385-390
ISBN: 978-989-8425-52-2
Copyright © 2011 SCITEPRESS (Science and Technology Publications, Lda.)



	Infrastructure as a Service				Platform as a Service				Software as a Service		
	Storage scalability	Computing scalability	Secure communication / virtual networks	Disaster Recovery	Data backup	Data integrity	Availability / Continuity of Service	Auditability	Patient empowerment / self management	Care newtorks and communities	Privacy Management
Grid Services for Clinical Research	■	■				■					
Virtual Healthcare Professionals network			■				▒	▒		■	▒
Consumer Health Informatics (e.g., PHR)	■		■		▒	▒		■	■	■	■
Electronic Health Record	■				■	■	▒	■	▒		▒
Health Knowledge management	■	■	▒		▒				▒	▒	
Remote Monitoring	■		■		▒	■	■		■	■	■
Healthcare Information Systems	■			■	■	■	■	■			

Figure 1: eHealth domains and Cloud services matrix.

healthcare providers that can be exported for use in other institutions. There are some standards that can be used for this purpose: HL7, ANSI X12, CEN, DICOM, etc. The EHR is important to ensure a good interoperability in the communication between medical structures thus resulting in the improvement in cost and time effectiveness within the healthcare system.

According to a report from marketing research firm Kalorama Information, the market for EHR systems will grow by 14.1% annually through 2012.

- **Health Knowledge Management:** is the implementation of an IT system that can support the creation, capture, retrieve, share and effective application of knowledge for the improvement in health. In 2005, WHO began a global initiative for the diffusion of the Knowledge Management Strategy aimed to implement programs capable of bridging the gap between knowledge and practice, the "know-do gap". ICT solutions could help in providing and retrieving always updated medical knowledge through the use of semantic technologies and ontologies.

- **Remote Monitoring:** (e.g., telemedicine, m-Health, Ambient Assisted Living, home healthcare, etc.): it includes all kind of remote communication of data among patient and healthcare professional, done through electronic resources. Some example of remote monitoring are telemedicine that allows treatment and care services given directly at the patient's home (sometimes called in a more generic term as "home healthcare"); m-Health, that includes the collection of data from devices; Ambient Assisted Living that provides all methods, concepts and electronic systems useful to support an assisted person.

- **Healthcare Information Systems:** it can be described as the core of the Hospital/Medical IT structure system. It's usually composed by the clinical data repository, clinical decision support system, checked medical vocabulary, computerized provider order entry, pharmacy management system, and the electronic medication administration record (like solutions for appointments and work schedule management).

This paper will explore the potentialities and limitations that the use of cloud infrastructures and platforms for the eHealth sectors. In particular, section 2 will describe the main drivers and opportunities that could lead to adoption of Cloud infrastructure from Health Organizations, while section 3 will underline some important aspects to take into account before opting for such choice.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

2 BENEFITS OF EHEALTH FROM CLOUD SOLUTIONS

As many other domains, eHealth could benefit a lot from the three main innovative infrastructural aspects (Armbrust et al, 2009) of cloud computing: the illusion of infinite computing resources available on demand, the elimination of an up-front commitment by Cloud and the ability to pay for use of computing resources. However there can be more specific advantages in the use of Cloud Computing solutions for the different sub-domains of eHealth mentioned above, as shown in Figure 1, that can be proposed at Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) levels. In particular, some of these domains' requirements are:

a) **IaaS - Storage Scalability:** Research from a global survey (BridgeHead 2010) from hospitals and healthcare organizations worldwide revealed that medical images, scanned documents, email and advances towards the EHR are going to be the cause for a meaningful increase in healthcare data that is already challenging hospitals. Most of the participants in this survey (41%) claimed that they are expecting an increase in the data volume up to 25%, while approximately one fifth of them (18%) is expecting a growth from 25% to 50%. Besides traditional Healthcare Information Systems, there are other emerging fields of eHealth that could lead to exponential growth in the database size. For example remote monitoring, especially if the patient's monitoring is continuous (regardless of the activity to be monitored, e.g., ECG, physical activity, etc.), and with a lot of patients, we can expect rapid expansion of the data volume. Cloud Computing allows to easily scale storage capacity when needed.

b) **IaaS - Computing Scalability:** Cloud Computing offers also computing power scalability which may be particularly important for some eHealth domains. One example is the Grid Services for Clinical Research. Health institutions which perform also clinical/medical research can have the need to perform analysis on large volumes of data, requiring also large computational power. However these studies are not continuous, which makes Cloud Computing particularly suitable for these applications, with its pay-per-use model. Another example may be the information search on large database of trusted medical knowledge. In this case, a lot of computing power may be needed if several users perform searches on journals, articles, etc. at the same time, but this is hard to predict in advance.

c) **IaaS - Virtual Networks:** An interesting IaaS feature that the Cloud could offer is the creation of virtual networks to connect healthcare institutions (like in the case of Virtual Healthcare Professionals networks), or to connect patients and healthcare institutions (like in the case of remote monitoring, e.g., telemedicine, AAL, etc.).

d) **IaaS - Disaster Recovery:** The results from BridgeHead survey reported what are the top priorities in the next investments for IT budget in healthcare organizations. Disaster recovery, together with Data Backup and Business Continuity, was a priority for 44.3% of the respondents. Cloud Computing could offer backups and redundancy at lower costs with respect to legacy systems.

e) **PaaS - Data Backup:** In line with the previous point, Data Backup is a top priority for many organizations. It was separated because Data Backup deals more with databases and data structure (PaaS level), while Disaster Recovery deals more with storages and virtualization (IaaS level).

f) **PaaS - Data Integrity:** Medical data integrity should be guaranteed to assure the correctness of the care process. This should be guaranteed both in Healthcare Information Systems and in possible EHR applications running on the Cloud.

g) **PaaS - Availability/Continuity of Service:** Business continuity and availability are very important in most of the medical applications, especially those dealing with possible emergency situations detection (e.g., remote patients' monitoring) and management (e.g., availability of the EHR in a dangerous situation). The main objection to the adoption of Cloud Computing (65%) in the BridgeHead survey was the hospitals' concerns about the security and availability of healthcare data given the great number of threats, including privacy breaches and identity theft. Other objections include cost (26.1%) and a lack of confidence that Cloud offers greater benefits with respect to local storage media (26.1%). In theory, Cloud solutions will assure better continuity than legacy systems, but on this Cloud Providers still need to convince their possible customers, as shown from the results of the BridgeHead survey.

h) **PaaS - Auditability:** The possibility to ensure that the IT system is compliant with existing regulations is very important for eHealth applications, in particular for what concerns the management of patients' data in accordance with privacy protection directives. PaaS type of services should ensure the auditability to attract Health Organization in investing in this kind of solutions. This is particularly critical for example in managing EHR or PHR applications, but also in case the Cloud will host and run Hospital Information Systems.

i) **SaaS - Patient Empowerment in Self-management:** One of the main driver for the adoption of Cloud Computing in eHealth can be the trend that sees the patients becoming more and more protagonist of their health management process (Mandl and Kohane, 2008). Thanks to the information and communication technologies, patient-doctor relationship is evolving and may be potentially resulting in more shared decision making process. A study conducted over 6369 persons claimed that almost two thirds (63.7%) of adults searched online for some type of health or medical information either for themselves or for someone else through the Internet. In general, evidence shows that, even if health professionals remain the most trusted source of Health information, electronic media are becoming more and more important too, and in some cases, patients are looking for information online before talking with their physicians (Hesse et al, 2005). In the new scenario just depicted, it clearly shows the limitations of the vision of EHR stored locally on an internal

Healthcare Organization database. Cloud Computing platforms at different levels of abstractions, could support this new paradigm of eHealth. The proposals of Google (with GoogleHealth) and Microsoft (with their Health Vault) of Health related SaaS platforms is a demonstration of the business opportunities and benefits of Cloud Computing applications in this domain.

j) **SaaS - Care networks and Communities:** SaaS solutions could also facilitate the shift from traditional EHR to Patient-Controlled Health Records (PCHR), as well as the creation of patients support networks and online medical communities, which are more and more a reality thanks to Web 2.0 technologies (Lo and Parham, 2010).

k) **SaaS - Privacy Management:** The possibility to manage privacy settings of personal data must be ensured for the success of SaaS solutions for eHealth. In particular this problem will be described in the next section. The access control to patients' data is not only role-based but also context-bases. For example, patient's relatives may have access to the patient's record in cases of emergency (in cases where data is required while the patient is unconscious and cannot provide his/her consent), but not in normal conditions. In the development of platforms that will make the exchange of medical data seamless and easy, patient must be sure that his/her data are treated not only according to national/international regulations, but also to their personal preferences.

Figure 1 shows a table with the eHealth domains and the requirements listed above. The cells have been coloured in dark gray to identify areas in which the adoption of Cloud Computing solutions can have a meaningful impact, while in light gray we indicated areas in which Cloud Computing is not critical to satisfy that requirement but can contribute to achieve it.

3 ANALYSIS AND LIMITATIONS OF THE EXISTING CLOUDS

Cloud Computing offers a lot of potential advantages to Health and eHealth applications as described in the previous section, however there are still several obstacles related to the adoption, the growth and the policy management of the Cloud. In particular the main problems are 1) availability of service, 2) data lock-in (and interoperability), the 3) data confidentiality and auditability, 4) data protection regulations compliance, and 5) security:

1) **Availability:** availability is a crucial issue for any company whose business continuity is critical, and Healthcare Organizations are a perfect example for this. Cloud providers should be able to demonstrate that they can guarantee the continuity of service in order to convince healthcare providers to move their systems to cloud. For example, unavailability of data is intolerable for Healthcare Organizations in case of the need to access patients' health records in critical situations or during an audit for certifications, etc. These questions are to be addressed by a recent FP7 project TClouds (TClouds, 2011) funded by the European Commission. The TClouds project proposes a solution that involves the creation of a federation of Clouds Providers to ensure availability and avoid single point of failure, in case one cloud provider in the federation has problems.

2) **Data Lock-in:** APIs for Cloud Computing itself are still essentially proprietary, or at least have not been the subject of active standardization (Armburst et al, 2009). The fact that healthcare organization cannot easily migrate their data and software from one Cloud Provider to another is a major implicit risk in the adoption of a cloud infrastructure. For example, Hospitals are required by law to keep medical records for a long period of time, and the "survival" of the Cloud Provider is not guaranteed (as in any new IT market, competitive pressure, inadequate business strategy, lack of financial support, etc, could lead some providers to go out of business or at least to force them to restructure their service portfolio offering).

3) **Data Confidentiality and Auditability:** As far as data confidentiality is concerned, it is more a psychological problem of not having the data under direct control but there is no reason to think that Cloud Infrastructure can't have the same security level of in-house applications. Many of the obstacles can be overcome immediately with technologies such as encrypted storage, VLAN etc. Encrypting data approach was successfully used by TC3, a healthcare company with access to sensitive patient records, when moving their HIPAA-compliant application to Amazon Web Services (Amazon, 2010). Besides standard security policies, Cloud Computing should consider additional risks like in the case of multiple tenancies and the reuse of hardware resources, where there is also a high risk due to insecure or incomplete data deletion (an important issue in medical cases). It's also critical to define system administrators and how to manage security by service providers, to avoid damage

caused by malicious insider: the risk is often greater than expected.

Furthermore, it is reasonable to expect even not malicious violation of data confidentiality, for example in case Cloud Providers observe data traffic in the Cloud for legitimate security protocols and procedures.

4) **Regulation Compliance:** it may be difficult for the health organization (in its role as data controller) to effectively check the data handling practices of the Cloud Provider and thus to be sure that the data is handled in a lawful way. As an example of privacy policies compliance, Google Health and Microsoft HealthVault both declared that their services aren't covered by the Health Insurance Portability and Accountability Act (HIPAA), whose privacy rules protect the privacy of individually identifiable health information, they don't store data on behalf of health care providers and their primary relationship is with the users (Microsoft, 2009; Google, 2010).

To support the growth of the use of these technologies ensuring protection of patient's privacy, the Health Information Technology for Economic and Clinical Health (HITECH) Act recently extended the requirements provided by HIPAA, also to the PHRs vendors. HITECH Act compliance is at the moment untested and presumably, the Google and Microsoft repositories are not aligned with it yet (U.S. Department of Health & Human Services, 2010; Gordon M., 2010). The TClouds project will identify legal constraints and privacy risks associated with cross-border cloud deployments. This analysis will drive the implementation of a federation of Clouds platform.

5) **Security:** The European Network and Information Security Agency (ENISA) provides some recommendations to prevent issues and risks related with Cloud Computing (Perilli A. et al, 2010). First of all Cloud customers need assurance that providers are implementing appropriate security strategies to mitigate security risks (they need this in order to make sound business decisions and to maintain or obtain security certifications). The parties of a contract should pay particular attention to their rights and obligations related to notifications of breaches in security, data transfers, creation of derivative works, change of control, and access to data by law enforcement entities. Moreover, they should carefully consider whether standard limitations on liability adequately represent allocations of responsibility given the parties' use of the cloud, or responsibilities for infrastructure. These issues are especially delicate if we consider that the medical data are sensitive data. How to build trust in the Cloud, data protection in large scale cross-organizational systems, and large scale computer system engineering (resource isolation mechanisms, interoperability, resilience, …), are priority areas of research in order to foster the adoption of Cloud Computing infrastructure both from traditional Healthcare providers and eHealth providers.

4 CONCLUSIONS

Healthcare infrastructures relies more and more on ICT infrastructures, thanks to continuous computerization of healthcare processes and digitalization of clinical documents. Furthermore, new trends in eHealth see more and more the patient as a proactive actor (and not anymore an object) of these processes. Cloud Computing seems to be a perfect solution supporting these trends, and providing cost-efficient and scalable solutions, however Cloud Providers should guarantee as commodity, important features of their platform like resiliency, auditability, privacy protection, compliance with regulations, etc.

As described in this paper, there are several "definitions" of eHealth and many of them can benefit from Cloud solutions at different levels. However this implies that very different actors should be convinced to invest in this kind of technologies, both as cloud providers and users, ranging from hospitals, care networks, National/Regional healthcare systems, big IT enterprises (e.g., Google, Microsoft), small/medium enterprises (e.g., telemedicine companies), etc. For this reason, it is hard to predict how the Cloud market will move in the next years and who will be the first adopters, even if some first solutions are already appearing and demonstrating sound business opportunities (e.g., Microsoft HealthVault).

As far as the European scenario is concerned, for the moment the emerging cloud computing market is already led by US players, which could lead to difficulty in compliance with European and national specific regulations. US centricity and lack of verifiable resilience and privacy are reasons why today's cloud infrastructures can only be used for applications that are neither business critical nor privacy sensitive. For this reason, many European eHealth businesses cannot benefit yet from the advantages offered by cloud solutions. While private clouds could be an answer in this sense, they will never reach economies of scale and scope that are needed to provide cost effective solutions.

In this sense, besides designing a platform to improve privacy and resiliency of existing Clouds, the TClouds project will also identify business and legal challenges, in order to build a regulatory framework for enabling privacy-enhanced cross-border infrastructure Clouds.

ACKNOWLEDGEMENTS

This research has been partially supported by the TClouds project http://www.tclouds-project.eu funded by the EU 7th Framework Programme ([FP7/2007-2013]), grant number ICT-257243.

REFERENCES

Amazon Web Service Case Study: TC3 Health. 2010. Retrived November 15, 2010, form http://aws.amazon.com/solutions/case-studies/tc3-health/

Amrhein, D., Quint, S. 2009. *Cloud computing for the enterprise: Part 1: Capturing the cloud*. Retrieved November 2, 2010, from http://www.ibm.com/developerworks/websphere/techjournal/0904_amrhein/0904_amrhein.html

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., Stoica, I., and Zaharia, M. 2009. *Above the Clouds: A Berkeley View of Cloud Computing*. Retrieved November 2, 2010, from http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

BridgeHead. 2010. *Report: The BridgeHead Software International 2010 Data Management Healthcheck Survey* Retrieved November 2, 2010, from http://www.bridgeheadsoftware.com/pdfs/BH_Rpt_Data-management-survey-results_A4.pdf

Google. 2010. *Google Health and HIPAA*. Retrieved November 15, 2010, from http://www.google.com/intl/en-US/health/hipaa.html

Gordon M. 2010. *HITECH Extends Privacy Obligations to EHRs and PHR Vendors*. Retrieved November 15, 2010, from http://www.itbusinessedge.com/cm/community/features/guestopinions/blog/hitech-extends-privacy-obligations-to-ehrs-and-phr-vendors/?cs=38631

Hesse, B. W., Nelson, D. E., Kreps, G. L., Croyle, R. T., Arora, N. K., Rimer, B. K., and Viswanath, K. 2005. *Trust and Sources of Health Information*. Arch Intern Med. 2005;165:2618-2624

Lo, B., and Parham., L. 2010. The Impact of Web 2.0 on the Doctor-Patient Relationship. *The Journal of Law, Medicine & Ethics*, vol. 38, Issue 1, (Spring 2010) pp.17–26

Mandl, K. D., and Kohane, I. S. 2008. *Tectonic shifts in the health information economy*. N Engl J Med 2008 Apr 17;358(16):1732-1737.

Markle Foundation. 2003. *The Personal Health Working Group Final Report*. Retrieved March 2, 2010, from http://www.connectingforhealth.org/resources/final_phwg_report1.pdf

Microsoft. 2009. *Microsoft HealthVault and HIPAA*. Retrieved November 15, 2010, from http://msdn.microsoft.com/en-us/healthvault/cc507320.aspx

Perilli, A., Manieri, A., Algom, A., Balding, C., Bunker, G., Rhoton, J., Broda, M., Rohr, M., Brian, O., Lindstorm, P., Dickman, P., Massonet, P., Samani, R., Pascoe, S., Nair, S., Balboni, S. 2009. *Benefits, risks and recommendations for information security*. Retrieved November 15, 2010, from http://www.enisa.europa.eu/

Tang, T. C., and Lee, T. H. 2009. *Your Doctor's Office or the Internet? Two Paths to Personal Health Records*, New England Journal of Medicine 360 (2009): 1276-1278.

TClouds. 2011. "Trustworthy Clouds". Retrieved February 25, 2011, from: http://www.tclouds-project.eu/

U.S. Department of Health & Human Services. 2010. *HITECH Act Rulemaking and Implementation Update*, Retrieved November 15, 2010, from http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechblurb.html

World Health Organization. n.d. *Department of Knowledge Management and Sharing (KMS)*. Retrieved March 2, 2010, from http://www.who.int/kms/en/