Privacy Impact Assessment Model for Deploying e-Health Applications in Cloud Transformations: Legal and Ethical Perspective

By

Iheanyi Samuel Nwankwo[*]

1. Introduction

One technological innovation of the 21st Century that has once again brought into focus the impact and extent of legal regulation of ICTs is cloud computing. In fact, many legal experts have even begun to refer to it as the 'cloud of unknowing'.[1] Although the concept is not new, the scale at which the infrastructure is being developed and projected makes it ground breaking after the discovery of the internet. Today, cloud computing could be compared with the power grid. Despite its perceived risks, the advantages of using cloud infrastructures and services appear too enticing to be resisted, and are forcing business organisations and even governments towards adopting this technology.[2] Gartner (2010) has projected that cloud computing will generate $ 148.8 billion by 2014, and organisations will save at least a third of their initial cost of maintaining an in-house IT department when they use cloud services.[3]

In a layman's understanding, cloud computing represents a business model where the traditional IT solutions of enterprises are outsourced to cloud service providers. In this model, organisations do not need to purchase IT equipment such as servers, software, storage facilities, and even maintenance services. These are outsourced to dedicated IT outfits that specialise in such services, thereby allowing organisations to deal with their core business objectives. This service provisioning is not limited to the business sector alone, even academic institution and non-profit organisations are also adopting it. The use of such computing capabilities is equally gathering momentum presently in the health sector as more e-health applications are being developed with the cloud in focus. Rial (2012) sees e-health as the next big step in cloud computing.[4] Bennett (2011) is also convinced that: "In cloud environment, multiple systems or servers can be launched at a fraction of the cost, time and effort of a manual deployment".[5] Stressing further that, "coordination of hardware, software and clinical transformations" are better managed in the cloud. Many other previous studies have reported the potential benefits of the use of cloud computing in improving healthcare services.[6] Rolim et al (2010) have proposed using a cloud-based system to automate the process of collecting patients' vital data via a network of sensors connected to legacy medical devices, and to deliver the data to a medical centre's "cloud" for storage, processing, and distribution.[7] This system will provide users with 7-days-a-week, real-time data collection, as well as eliminates manual collection work and typing errors.

Not only are private entities promoting this service offering, public authorities are also encouraging initiatives that will make use of cloud infrastructures in the health sector. In Australia for instance, an e-health cloud is being proposed that will host healthcare applications

[*] Institute für Rechtsinformatik, Leibniz Universität Hannover. Email: nwankwo@iri.uni-hannover.de

[1] Kuan Hon, Christopher Millard and Ian Walden 2011, 'Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2', Queen Mary School of Law Legal Studies Research Paper No. 77/2011.

[2] See for example, European Commission, 'Unleashing the Potential of Cloud Computing in Europe', COM (2012) 529 final.

[3] 'Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010', available at: http://www.gartner.com/it/page.jsp?id=1389313.

[4] Nerea Rial, 'e-Health, the Next Big Step for Cloud Computing', New Europe online, 17 April 2012, available at: http://www.neurope.eu/article/e-health-next-big-step-cloud-computing.

[5] Stephen Bennett, 'Cloud Computing and Electronic Health Records: New Trend?' Computerworld, 3 January 2011, available at: http://blogs.computerworld.com/17538/cloud_computing_and_electronic_health_records_new_trend.

[6] Ibid.

[7] Carlos Rolim et al 2010, 'A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions', available at: http://www.healthlawyers.org/Members/PracticeGroups/HIT/Toolkits/Documents/Cloud%20Computing%20Resource%20Toolkit/2_ArticlesAndPapers/Rolim-Cloud_Computing_Solution_for_Patient%27s_Data_Collection%20in%20Health%20Care%20Institutions.pdf.

including clinical software, decision-support tools for diagnosis and management, care plans, referral tools, prescriptions, training, and other administrative and clinical services.[8] Various European Union funded projects such as p-medicine, OPTIMIS, epSOS project, Tcloud, VPH Share, etc, also aim at utilising cloud transformations for e-health applications.

In spite of the advantages of using cloud computing in the health sector, a deeper analysis of this shift from the tradition IT paradigm, where healthcare providers used to own their servers and manage their computing capabilities may be required before deploying e-health applications. This is because processing and storing of sensitive health-related data in the cloud present huge challenges for data controllers in view of the complex web of regulatory and compliance requirements they are meant to observe. Cloud computing introduces new security threats and vulnerabilities that are not present in the traditional IT environments.[9] This is not only as a result of the borderless nature of the cloud architecture, but also the heightened risk of the whole scale outsourcing that usually follows its service offerings. This has the tendency of depriving the data controller the actual control of the data in most cases.[10] In fact, many commentators including privacy commissioners have voiced out concern about this innovative technology, and have even questioned whether cloud computing can ever be compliant with the current data protection regime in the EU.[11] There are obvious risks of losing the control of sensitive personal data involved in healthcare delivery in such computing outsourcing. In the traditional environment, the ability to layer stronger authentication, access control and auditing capabilities exist as a result of the defined network layers and physical control of infrastructure. By contrast, it has been argued that public clouds lack this clearly defined network layers, and present heightened opportunities for breaches of protected health information because of the nature of the infrastructure itself.[12] Not only are public cloud resources dynamically provisioned, data can be stored in any part of the world including states without adequate level of personal data protection. Thus, guaranteeing data security and integrity controls in cloud transformations may pose some obstacles in certain instances.

In this paper, we will examine the legal and ethical context under which e-health computing capabilities can be outsourced in the cloud. We will attempt to identify some, legal and ethical risks and challenges that may militate against the use of cloud in deploying e-health applications. We will also address these risks with the ultimate goal of proffering a risk assessment tool that will guide data controllers and data protection authorities in this regard. This paper is broadly divided into two parts. The first part looks at the basic concepts and issues surrounding cloud computing, including its benefits and risks in the health environment. The second part assesses a proactive risk impact model that will aid data controllers before deploying their e-health applications in the cloud.

2. Basic concepts and issues

2.1 The nature of cloud computing and its transformations

a. Cloud computing

Like most technical concepts, defining cloud computing is not without fraught difficulties as a result of the evolving nature of the technology. But for our purposes here and in a simply layout, cloud computing describes a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space.[13] A

[8] Alex Mu-Hsing Kuo 2011, 'Opportunities and Challenges of Cloud Computing to Improve Health Care Services', Journal of medical internet research, Vol 13, No 3 (2011), available at: http://www.jmir.org/2011/3/e67/.

[9] Sunil Pandey 2012, 'Cloud Computing: Security, Privacy & Ethics', available at: http://developeriq.in/articles/2012/sep/01/cloud-computing-security-privacy-ethics/.

[10] See the Article 29 Working Party, WP 196, Opinion 05/2012 on Cloud Computing, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

[11] Fance, Italy, Uk, and Germany Data Protection Authorities have issued opinions on cloud computing.

[12] Peter Mell and Timothy Grance 2011, *Guidelines on Security and Privacy in Public Cloud Computing,* available at: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

[13] Article 29 WP 196, op. cit., p. 4.

more technical and widely cited definition by the United States National Institute of Standardisation and Technology (NIST) defines the concept thus:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[14]

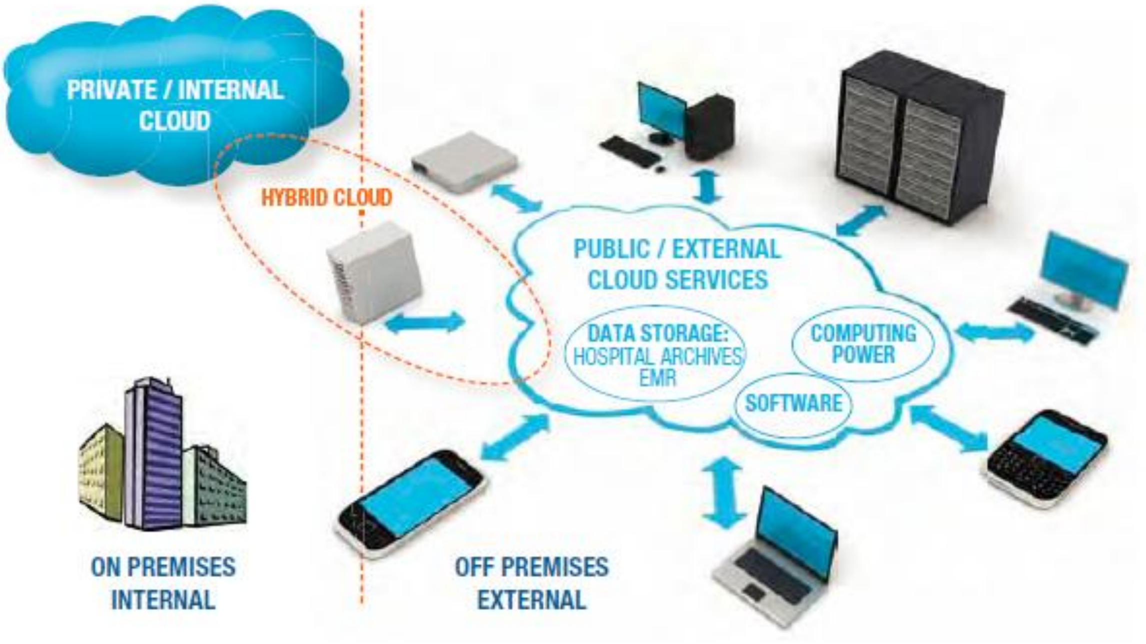
These service models can be offered as *Software as a Service (SaaS)* in the form of providing the cloud service consumer with the capability to use the cloud service provider's applications (software) running on a cloud infrastructure.[15] These applications are configured to suite the consumers preferences and are accessible from various client devices through the Internet (e.g., web-based email, electronic health records). *Platform as a Service (PaaS)* is another service model that is found in the cloud where the service consumer is provided with the capability to deploy onto the cloud infrastructure applications created using programming and support tools by the service provider (e.g., centralised analysis of MRI scans or X-rays built for example on Microsoft Azure). *Infrastructure as a Service (IaaS)* refers to the capability provided to the service consumer to provision processing, storage, networks, and other fundamental computing resources, as well as being able to deploy and run arbitrary software. These can include operating systems and applications (e.g., networks for transmission of diagnostic tests or the inputs from personal monitoring devices).[16]

One fundamental consequence of these service models is that the service consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage,[17] but may have control over the deployed applications and possibly configuration settings for the application-hosting environment.[18]

b. Cloud transformations

Services offered in the cloud could be deployed in four possible ways, namely:
Private cloud, where the cloud infrastructure is provisioned for exclusive use by a single organization. It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.[19] This model is comparable to buying, building and managing your own infrastructure. It is more beneficial for security purposes and may not bring much in terms of cost efficiency.[20]
Community cloud, where the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
Public cloud, where the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
Hybrid cloud, where the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).[21]

[14] Peter Mell and Timothy Grance 2011, *The NIST Definition of Cloud Computing*, available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
[15] Ibid.
[16] Ibid.
[17] This is the case in public clouds, but may vary in private clouds.
[18] Peter Mell and Timothy Grance, op. cit.
[19] Ibid.
[20] Neeraj Metha 2012, 'The 4 Primary Cloud Deployment Models', available at: http://www.cloudtweaks.com/2012/07/the-4-primary-cloud-deployment-models/.
[21] Peter Mell and Timothy Grance, op. cit, p.3.



Source: COCIR e-health toolkit 2012

c. Benefits and risks

Much ink has flown and is still flowing on the benefits and risks of using cloud business model. These range from technical to business outlook of the innovative technology. The benefits of cloud infrastructures are still emerging. It is the scalability of using the Internet for its service delivery that is the most promising attribute of the technology that reduces cost and allows for accessibility no matter the location and time. Generally, the benefits of using cloud computing include:

a, cost reductions: the use of cloud infrastructure relives consumers the hassles of purchasing their own IT equipments such as servers, storage facilities, software etc, and can pay according to the capacity they used (pay-per-use). Organisations using cloud technology have reported huge cost reduction not only from maintenance, but also from acquisition of devices and installation equipments.[22]

b, scalability and flexibility of service: not only do cloud services used only when they are needed, additional capacity could be requested within seconds to meet any compute upsurge. Thus services can be 'bursted' to cater for extra needs without the hassles of investing in new equipments and installation.

c, increase security due to large scale: it has been argued that using cloud infrastructure could increase the security standing of small and medium sized businesses who may not have the resources to upgrade to the state of the art information security tools.[23]

d, automatic maintenance and updating: cloud service providers take care of the maintenance of the IT resources and updating of the underlying software. This relieves organisations using cloud infrastructure the cost of keeping huge IT department for maintenance.

e, device independence: cloud computing allows accessibility through multiple devices such as mobile phones, tablets, computers etc, so that when changing device, existing applications are still available. There is no need for a special version of a program for a particular device, or to save a document in a device-specific format.[24]

[22] Lisa Boch- Anderson 2011, , Hospital uses cloud computing to improve patient care and reduce costs', available at: http://www.microsoft.eu/cloud-computing/case-studies/hospital-uses-cloud-computing-to-improve-patient-care-and-reduce-costs.aspx.

[23] The Backup List 2012, 'Is The Cloud Really A Security Risk?', available at: http://www.thebackuplist.com/is-the-cloud-really-a-security-risk/.

[24] The European Parliament 2012, *Cloud Computing Study,* available at: http://ec.europa.eu/information_society/activities/cloudcomputing/docs/cc_study_parliament.pdf, p.34.

However, in spite of the above benefits, there are also inherent risks in adopting cloud computing. The Article 29 Working party has outline these risk in its opinion suggesting that data protection and privacy risks as a result of loss of control over personal data by the data controller, as well as lack of transparency as to the nature data processing are the main risks in using the cloud.[25] There are possibilities that this loss of control by the data controller can lead to the breach of the data protection law applicable to the controller, which in most cases may span within multiple jurisdictions.[26]

Furthermore, despite the ability to implement sophisticated security tools in the cloud, there is the concern that cloud computing presents a heightened threat to data security due to the concentration of data on common cloud infrastructure.[27] Data are more susceptible to be compromised due to the multitude of actors and sub-processors involved in the service. Each layer of the stack may involve services provided by a different cloud provider or even third party.[28] There is also the concern that because of service delivery via the Internet, access is cut off whenever the Internet connection breaks.

Apart from the above, no knowing the geographical location of service provisioning, vendor lock-in, unequal contract negotiating power, lack of standardisation in cloud architecture and access to data by law enforcement agencies without the knowledge of the data controller have all been conversed as part of the risks of the cloud technology. In the subsequent sections, we will look at these specific risks as they affect e-health cloud services.

2.2 E-health and the use of cloud computing

a. The nature of e-health and its cloud applications

The modern day healthcare needs and delivery is complex, and the use of ICTs has made some positive impact in attending to such needs that e-health applications require. These range from recording health information in electronic formats to making such record available at any time and place; to seamlessly interoperating the various e-health applications and the provision of the enormous compute and storage capabilities of the modern healthcare delivery. E-health**,** which simply stands for the application of ICTs across the whole range of functions that affect the health sector - from the doctor to the hospital manager to the patients,[29] has brought a new paradigm in healthcare delivery. New ICTs have the potentials to revolutionise healthcare and health systems and to contribute to their future sustainability.[30] In fact, the European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry (COCIR) has itemised the benefit of e-health in their recent e-health toolkit, which include medical cost reduction, improve and secure transfer of patient information, and facilitation of easy access to healthcare among others.[31]

Cloud computing appears well suited in bringing e-health to the next level because of its alignment with the e-health objectives such as interoperability of ICT facilities and seamless integration of data. "It can link doctors to hospitals, labs, insurers and to patients in new ways that even the most 'wired' healthcare systems are only beginning to explore today".[32] And as indicated earlier, the use of cloud in deploying e-health applications has been gaining much recognition and predicted to be worth $5.4 Billion by 2017.[33] KLAS (2012) recently conducted a

[25] Article 29 WP 196, op. cit.
[26] Nikita Anand 2010, 'The Legal Issues Around Cloud Computing', available at: http://www.labnol.org/internet/cloud-computing-legal-issues/14120/.
[27] The European Parliament 2012, op. cit, p.9.
[28] Dave Krebs 2012, 'Regulating the Cloud: A Comparative Analysis of the Current and Proposed Privacy Frameworks in Canada and the European Union', 10 Canadian Journal of Law and Technology 29 (Carswell), p.35.
[29] Euractiv 2010, 'e-Health', available at: http://www.euractiv.com/health/ehealth-linksdossier-188197.
[30] European Commission 2007, 'Together for Health: A Strategic Approach for the EU 2008-2013', COM(2007) 630 final, available at: eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0630:FIN:EN:PDF.
[31] COCIR 2012, *COCIR eHealth Toolkit Contributing to the European Digital Agenda*, 2nd ed, available at: http://www.cocir.org/uploads/documents/-1523-ehealth_toolkit_2012.pdf.
[32] Microsoft 2009, *Towards a Healthier Europe*, available at: http://www.euinnovationday.com/pdf/eHealth.pdf, p. 4.
[33] Florence de Borja 2012, 'Cloud Computing Health Care Market Worth $5 Billion by 2017' available at: http://cloudtimes.org/2012/07/18/cloud-health-care-market/.

survey of small clinics and hospitals and surprisingly found that 55% are already using cloud-based apps.[34] The COCIR puts it even clearer:

> Cloud computing offers similar benefits for the health industry, driving down costs, making administrative processes leaner and more efficient, reducing the time needed for patients to interact with health workers and providing increased access for patients to their health records. The cloud model also offers benefits specific to the health industry. It will allow healthcare companies, researchers and healthcare workers to share expertise, advance research through online collaboration and visualise, through geographic mapping, where problems are located, evaluate trends and health risks, and identify regions or municipalities not receiving satisfactory care.[35]

In practical terms, the use of cloud in the health sector has been recorded in a number of cases that are worthy of comment. In 2011, Brainlab launched its VoyantLink which is a cloud platform that allows access, sharing and viewing of patient diagnostic images between hospital staff and surgeons.[36] This service is an enrichment cloud framework between clinicians, hospitals and imaging centers that allows users to create a workspace unit that employs clinical management tools and place them on completed tasks to any device or data location that can be accessed by all people on the patient management team, thereby making collaboration and updating quick and easy. Similarly, AT&T is hosting a Medical Imaging and Information Management (MIIM) cloud service that will allow sharing of files like MRI and X-ray results between doctors using a special cloud platform.[37] By 2012, it is expected that there will be billions of images stored in this platform for professional access.

In the UK, the Edinburgh Napier University and other partners have developed a cloud solution for the large scale deployment of sensitive medical data under the Data Capture and Auto Identification Reference (DACAR) project.[38] This e-health cloud platform allows the capture, storage and consumption of sensitive healthcare data for the development and integration of time critical e-health services such as the Early Warning Score (EWS). DACAR's e-health platform belongs to the *PaaS* category, but uses *IaaS* to establish a scalable and cost-effective cloud infrastructure. Secondly, it provides a solution stack to facilitate the development, integration and deployment of e-health *Software as a Service*.[39] Apart from the above examples, many public cloud service providers such as Microsoft, Dell, Google, Amazon, etc have developed specific infrastructure for the health sector such as Microsoft HealthVault,[40] and the Dell Secure Healthcare Cloud.[41] Below, we will look at the specific benefits and risks of using cloud infrastructure in deploying e-health applications.

b. Outsourcing e-health in clouds: benefits and risks

While our general discussion on the benefits and risk of cloud computing applies equally to the e-health cloud such as driving down costs and providing a more efficient way for patients to access their records and interact with health workers,[42] the cloud models also offer benefits specific to the health industry. In this section, we will highlight some of the specific contexts in which cloud computing apply in the health sector. The modern healthcare provisioning is complex: requiring integration of large amount of data from various sources in order to solve

[34] See Cloud Times 2012, 'Cloud Computing Implementation in Healthcare – Survey', available at: http://cloudtimes.org/2012/01/19/cloud-computing-implementation-on-healthcare/.

[35]Ibid.

[36] Irmee Layo 2011, 'Voyantlink from Brainlab Offers New Features for Surgeons', available at: http://cloudtimes.org/2011/11/28/voyantlink-from-brainlab-offers-ai-features-for-surgeons/.

[37] Irmee Layo 2011, 'Alabama and Michigan Hospitals to Innovate Medical Imaging Cloud', available at: http://cloudtimes.org/2011/06/27/alabama-and-michigan-hospitals-to-innovate-medical-imaging-cloud/.

[38] L. Fan, et al 2011, 'DACAR Platform for eHealth Services Cloud', available at: http://researchrepository.napier.ac.uk/4288/1/DACAR_IEEE%5B1%5D.pdf.

[39] Ibid.

[40] See http://www.microsoft.com/en-gb/healthvault/default.aspx.

[41] See http://content.dell.com/us/en/enterprise/healthcare-secure-healthcare-cloud.

[42] Lisa Boch- Anderson, op. cit.

complex health issues. Personalized medicine for example may require the continuous monitoring of patients in real time. Ranging from integrating healthcare information systems to performing analysis on large volumes of data from clinical and laboratory experiments, cloud computing is best suited for the modern day healthcare delivery: for it can offer the high performance computing as well as large storage space needed for this task. This is also beneficial in medical research and creation of virtual networks to connect healthcare institutions. The cloud equally makes it easy to connect patients and healthcare institutions (like in the case of remote monitoring, e.g., telemedicine, AAL, etc.).[43]

The cloud also offers improved communication, since access to health record will be available no matter the location, has the tendency to reduce both diagnostic and prescriptive errors.[44] Availability of EHRs even in cases of national disaster is part of the benefits identified by the adoption of cloud computing in the health sector.[45] COCIR (2012) has also identified the following benefits of cloud computing in healthcare:

- Cost reduction and increase efficiency in health services;
- Improved case management and rapid access to information by patients and medical team;
- Acceleration of business intelligence and data visualization;
- Enhanced security safeguards;
- Access to cloud expertise in terms of specialized services such as computing power.[46]

Nevertheless, new technologies must be evaluated properly as they are not without risks. The use of cloud technology in healthcare provisioning also has its own shortcomings. In the first place, there is lack of standardization in this area as it is still an emerging technology. Data portability and interoperability standards are not yet defined in the cloud and this may result to customer lock-in.[47] Data protection and security risks also come along with cloud-based deployment models. In certain cases, it is hard for a cloud service user (as data controller) to check the data management practices of a cloud service provider.[48] This may result in violation of legal obligations with grave consequences. Furthermore, it is not certain how to ensure availability when the internet connection is broken,[49] in view of the critical nature of e-health applications which in some cases require the monitoring of patients 24 hours continuously or in emergency situations.[50]

2.3 *Legal and ethical perspective of deploying e-health applications in cloud transformations*

a. Data protection and privacy issues

As shown in the preceding sections, cloud computing has revolutionised how IT infrastructures are provisioned, and promises greater advantages when adopted fully. However, some of the basic features of its technical and business model seem to be at odd with data protection laws. This has reoccurred as one of the basic challenges towards its adoption. While admitting that even in the traditional IT model, electronic processing of personal data presents some risks; such may be doubled when the process is outsourced to cloud providers as a result of the number of persons that handle data. The current data protection regime was framed to cater for the multiple intermediaries and frequency of transfers in the cloud, unlike the tradition

[43] Marco Nalin, Ilaria Baroni, Alberto Sanna 2011, 'e-Health drivers and barriers for Cloud Computing adoption', available at: http://www.eservices4life.org/administrator/components/com_jresearch/files/publications/e-Health%20drivers%20and%20barriers%20for%20Cloud%20Computing%20adoption.pdf, p.3.

[44] Mercedes Potter 2012, 'Cloud-based EHR Takes the Health Industry by Storm' http://bx.businessweek.com/cloud-cmputing/view?url=http://www.cloudbusinessreview.com/2012/06/19/cloud-based-ehr-takes-the-health-industry-by-storm.html.

[45] Ibid.

[46] COCIR 2012, op. cit., pp. 11-13.

[47] Ibid.

[48] Carlene Masker 2012, 'The Risks of Moving to the Cloud', available at: http://www.cloudtweaks.com/2012/09/the-risks-of-moving-to-the-cloud/.

[49] Emazzanti, 'The Dark-Side of Cloud Computing', available at: http://www.emazzanti.net/the-dark-side-of-cloud-computing/.

[50] 'Amazon Server Outage Raise Questions for Cloud in Health IT', available at: http://seekingalpha.com/instablog/856297-healthcare-capitalist/175466-amazon-server-outage-raise-questions-for-cloud-in-health-it.

framework which is defined and could be traced from point to point. Kerb explains that "it [data protection law] was, therefore, not designed to necessarily accommodate situations where personal data is moved freely from one jurisdiction to another (often unbeknownst to the individual), accessed over the Internet or where it shares server space with other parties, all of which may be the case where an organisation stores data with a cloud service provider." This state of affairs has generated a lot of comments and concerns from many quarters on how to squeeze cloud computing into the existing legal framework, especially, where sensitive data are involved. Within the EU, almost all the DPAs have made an opinion on the legal aspect of cloud computing. Below, we will examine these concerns as related to sensitive health-related data.

I. Threat to sensitive personal information

The way in which an e-health application is deployed in the cloud is of crucial importance to the nature and extent of the related privacy concern. For instance, it has been generally recognised that public clouds are confronted with more security challenges, and thus more difficult to guarantee the security of data deployed in a public cloud.[51] This assertion is made stronger by virtue of the feature of a public cloud that optimized resource through multi-tenancy and multiple third parties that participate in the service provisioning.[52] These multiple actors can also form weak links in the cloud. Cloud services sometimes involve stacking, whereby each layer of service may be provided by a different service provider and/or sub-provider. Each of these parties may form a weak link from where data breach may occur.[53] With each layer of abstraction, the data subject and/or data controller may further loss control of data to the cloud providers. The Article 29 Working Party has identified lack of control and transparency as the greatest challenge of data controllers in deploying data to the cloud. When data are processed on a machine that is owned by an entity different from the data controller such as in IaaS, there is a diminished guarantee that the processor will process data only on the instructions of the data controller. What this translates to in fact is that there is a high tendency for a third party to gain unauthorized access to data that is hosted in a public cloud, which may include personal data. This may happen without the knowledge of both the data subject and the controller. Even when the access seems lawful, for example, by law enforcement agencies, there are usually no guarantees that the concerned parties are informed.

One other consequence of cloud computing services is that it is location agnostic. Its architecture allows for dynamic provisioning of data and resources in a manner that makes nugatory the tradition boundaries upon which most data protection regimes were built. For instance, data sets (or sub-sets) may move from one jurisdiction into another jurisdiction within a millisecond depending on the virtual space available on a server.[54] This has some repercussions on the current data protection laws as applicable in EU member states which lay much emphasis on the location of data, and in most cases, expressly prohibit the transfer of personal data to third countries without adequate data protection, except where any of the legal exceptions permits. This state of affairs is worsened by the unfavourable contract terms that are used in most cloud offerings.[55] The imbalance in the negotiating power of the parties makes the cloud consumer weak and he either takes the offer or leaves it.

II. Data security

The security risks pertaining to cloud-based services are yet to be fully documented. However, the risk of centralisation of data and single point of failure cannot be overlooked. In most cases, multiple devices and access points also create some weak links for data breach.

Apart from the above, a cloud service provider has physical machines and computing resources located at some physical location, the security of which also is not guaranteed in terms of

[51] B. Kandukuri, V. Paturi, and A. Rakshit 2009, "Cloud Security Issues," in Proc. of SCC '09. IEEE, pp. 517–520.

[52] Sunil Pandey, op. cit.

[53] Dave Krebs, op. cit.

[54] Axel Spies 2011, 'Global Data Protection: Whose Rules Govern?', The Sedona Conference Journal, p. 107.

[55] Simon Bradshaw, Christopher Millard, Ian Walden 2010, 'Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services', Queen Mary School of Law Legal Studies Research Paper No. 63/2010, available at SSRN: http://ssrn.com/abstract=1662374 or http://dx.doi.org/10.2139/ssrn.1662374.

disaster recovery.[56] Cloud-specific security risks also relate to shared resources, which allow the same physical infrastructure to be used to serve many different customers of a cloud provider.[57] This in effect, means ceding control of security to some extent to the cloud service provider, but it is not entirely clear how the data controller would ensure that cloud service provider complies with the security requirements as required by the Data Protection Directive.[58]

Apart from privacy and security issues mentioned above, Kuo (2011) has identified other management and technical challenges such as bankruptcy and recoverability of data. The recent closure of Google Health, a cloud application service that aimed at giving free access to people to store their personal health and wellness information further brings an insight into the risk of adopting public cloud services for sensitive data processing. How would users of this service either recover their data as well as be sure that their data have been erased when the service finally goes offline? How can they circumvent the barriers in data, application and service interoperability in the cloud or are they simply locked-in? While this paper will not go into detail on the technical aspects of cloud computing, it is worthy of mention that uncertainties and lack of transparency are present in the cloud framework such as abrupt failure of services.

b. Medical ethics and the cloud

Cloud computing is evolving faster than regulation. However, there is an increasing need to apply some ethical values in its service offerings, most especially in the health sector in order to protect patients' safety and privacy. Sensitive health-related data in most cases hold the key to life and death. Where such data are compromised, they may cause irreparable loses to the data subjects such as employment and insurance opportunities. The pertinent question to ask in this respect is whether ethics should be a considerable factor before deploying e-health application in the cloud. Some commentators have even argued that certain sensitive or critical applications should not be deployed to the cloud. How will it be guaranteed for example, that the cloud service provide will keep medical records for a period of time required by law if goes bankrupt?[59] Will it be easy to transfer these data to a different provider in view of the lack of interoperability that exits in the services? Bannerman (2010) for instance, has made a cluster of 10 related cloud risk factors.[60]

From an ethical point of view, it is not clear whether patients are fully aware of the risks involved in processing their health data in the cloud, and have given an informed consent for such processing. Needless to say that involving non-health care practitioners in healthcare services through the outsourcing of support technologies raises some ethical questions as to: whether mere convenience in such outsourcing can be justified beyond patients'/public interest. Would it not heighten the risk of breach of confidentiality in the fiduciary relationship that exists between healthcare providers and their patients? The International Working Group on Data Protection in Telecommunications (2006) has indeed recognised this conflict, and maintained that:

> The special sensitivity of health information has to be kept in mind when considering the online availability of electronic health records. Under the Hippocratic Oath, doctors have always had to treat patients' information confidentially. To care for the health and the life of the patient has

[56] Rey Sveinsson, 'Cloud Computing and Security Concerns', available at: http://riskmanagementstudio.com/index.php/rm-studio-blog/211-cloud-computing-and-security-concerns?goback=.gde_2988428_member_166733727.

[57] European Commission 2012, 'Unleashing the Potential of Cloud Computing in Europe - What is it and what does it mean for me?', http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/713&format=HTML&aged=0&language=EN&guiLanguage=en#footnote-1.

[58] See Article 17 of the Data Protection Directive.

[59] Marco Nalin, Ilaria Baroni, Alberto Sanna, op. cit.

[60] Paul Bannerman 2010, 'Cloud Computing Adoption Risks: State of Play' in Proceedings of the 17th Asia Pacific Software Engineering Conference Cloud Workshop. New York, NY: IEEE; 2010:10-16, available at: www.nicta.com.au/pub?doc=4387.

> never been a licence to disclose such information to third parties who are not participating in the treatment of the individual patient.[61]

This position also finds a practical application in the e-health cloud outsourcing. From both legal and ethical perspective, it appears pertinent that consents must be obtained in order to legitimise data movement to the cloud. In the first instance, the Data Protection Directive requires an explicit consent from the data subject concerning the (further) processing of sensitive personal data, which is the case with the movement of data in the cloud from the hospital database.[62] Furthermore, an unambiguous consent from the data subject is also required concerning the transfer of data to third countries, unless exceptions apply.[63]

Furthermore, the Medical Device Directive may have some bearing on our subject matter. Although the 'cloud' is not a medical device under the Directive, medical software proposed as a service on the cloud (SaaS) are covered by the Directive if intended to be used for medical purpose. In this case, the cloud service provider needs to ensure that the software services comply with the essential requirements of safety and performance.[64] Where the cloud service provider is located outside the EU, and who in most cases may not be aware of the requirements, enforcement may be difficult.

3. Assessing cloud risks in a proactive model

While the current Data Protection Directive was drafted prior to the exponential growth of Internet enabled technologies, and did not take care of most of the privacy risks involved in their use, the European Commission has shown a strong determination to ameliorating these shortcomings. In a recent proposal for a new data protection regulation, the Commission recognised the risks involved in the processing of special categories of personal data including health-related data, and proposes to impose a proactive obligation on data controllers/processors of such data. In effect, they are to carry out a privacy impact assessment prior to the data processing. The Article 29 Working Party has also concluded in its recent opinion that businesses and administrations wishing to use cloud computing should conduct, as a first step, a comprehensive and thorough risk analysis designed to minimise two principle risks common to cloud services: lack of control and lack of transparency.[65] Similarly, the Norwegian Data Protection Authority also makes a thorough and good risk analysis a condition precedent for enterprises planning to move to the cloud.[66] While such a proactive measure is a welcomed development, however, no tangible standard has yet emerged for this assessment.[67]

a. Privacy impact assessment for e-health cloud

Cloud computing offers a lot of advantages to the health sector. It should however be noted that the transition to an outsourced, public cloud environment is in many ways an exercise in risk management, which entails identifying and assessing risk, and taking the steps to reducing them to an acceptable level. This can be a challenge in the cloud from deployments throughout the system lifecycle.[68] Although there have been various studies on the use of e-health applications

[61] The International Working Group on Data Protection in Telecommunications 2006, *International Documents on Data Protection in Telecommunications and Media 1983 – 2006*, available at: http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt.

[62] While it may be argued that Art. 8(3) of the Data Protection Directive permits the processing of sensitive data for the management of health-care services, which for instance may include cloud processing, it may not be the case that cloud service providers fall under health professionals subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

[63] Article 26 (1) (b) of the Data Protection Directive.

[64] COCIR 2012, op. cit., p. 13.

[65] Article 29 Working Party, WP 196, op. cit., p. 4.

[66] Norwegian Data Protection Authority 2012, 'Use of cloud computing services', available at: http://www.datatilsynet.no/English/Publications/Use-of-cloud-computing-services/.

[67] The DPAs of France, Italy, UK, Ireland have also issues some guidelines on cloud computing, indicating the need for a prior risk assessment before deployment.

[68] Sunil Pandey, op. cit.

in the cloud, there is a wide gap of academic knowledge as to the specific risks associated with deploying such applications in various cloud transformations from data protection and ethical prism. Thus, integrating such an assessment as a mandatory requirement if the proposed regulation takes effect, will be a proactive approach that incorporates risk management tools right from the start of any 'risky' data processing.

Privacy impact assessment is has been variously defined. Essentially, it is a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme and finding ways to mitigate or avoid any adverse effects.[69] Stewart (1996) has suggested that a PIA may be desirable in three main situations, namely to: assess risks from new technology or the convergence of existing technology; assess risks where a known privacy intrusive technology is to be used in new circumstances; and to assess risks in a major endeavour or change in practice having significant privacy risks.[70]

Various commentators and institutions have recognised the risks associated with the offerings and this makes it germane for a PIA to be carried out when sensitive data are to be deployed. The European Network and Information Security Agency (2009) has generally looked at the benefits and risks of cloud computing and has made recommendations regarding its security.[71] Kuo (2011) proposes SWOT (strengths, weaknesses, opportunities, and threats) as a healthcare cloud computing strategic planning model, though his analysis did not take specific account of legal and ethical factors from a EU perspective.[72] Bannerman (2010) also assessed cloud adoption risks generally, without specific focus on e-health applications.[73] This research however, seeks to bridge this gap.

Generally, there is no simple formula for the conduct of a PIA. Each PIA should be dictated by the specific institutional, technological, and programmatic context of the initiative in question.[74] However, in some jurisdictions, an official PIA template, format or other tool to describe how they should be conducted, is provided such as in the United Kingdom and Canada. Similarly, there are industrial specific PIAs such as the ISO 22307:2008 standard for PIA in the financial sector when data are being processed by automated, networked information systems.

Apart from these general approaches, the Health Insurance Portability and Accountability Act (HIPAA) in the US which seeks to the improve efficiency of the healthcare system and safeguard confidential personal health information, specifically provides that entities processing health information should "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."[75]

4. Future Research

Having identified some of the perceived benefits and risks of using cloud computing in deploying e-health applications, the future of this thesis will be to develop a standard model for conducting a privacy impact assessment as will be required by the new data protection regulation when it becomes enforceable.[76] So far, no model has been developed, but research is still ongoing that aims at analysing existing approaches and adapting them into a framework that will take

[69] See David Wright 2011, 'Should privacy impact assessments be mandatory?', *Communications of the ACM*, Vol. 54, No. 8, available at: http://cacm.acm.org/magazines/2011/8, p. 2.

[70] Blair Stewart 1996, 'Privacy impact assessments', [1996] PLPR 39, available at: http://www.austlii.edu.au/au/journals/PLPR/1996/39.html.

[71] European Network and Information Security Agency 2009, Cloud Computing: Benefits, Risks and Recommendations for Information Security, available at: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

[72] Alex Mu-Hsing Kuo 2011, 'Opportunities and Challenges of Cloud Computing to Improve Health Care Services', Journal of medical internet research, Vol 13, No 3 (2011), available at: http://www.jmir.org/2011/3/e67/.

[73] Paul Bannerman 2010, 'Cloud Computing Adoption Risks: State of Play' in Proceedings of the 17th Asia Pacific Software Engineering Conference Cloud Workshop. New York, NY: IEEE; 2010:10-16, available at: www.nicta.com.au/pub?doc=4387.

[74] Linden Consulting Inc. 2007, *Privacy Impact Assessments: International Study of their Application and Effects*,, Prepared for the Information Commissioner United Kingdom.

[75] 45 C.F.R. § 164.308(a)(1)(ii)(A).

[76] See Article 33 of the draft Data Protection Regulation.

account of the broader set of community values and expectation about ethics, privacy and security of sensitive health-related data.

5. Conclusion

Cloud computing is a tool that can accelerate innovation, cost-efficiency and modernisation in healthcare, but its development so far lacks transparency to transfer control to the cloud service providers without a proper risk assessment. It is not in doubt that cloud solutions can help healthcare providers in addressing healthcare challenges more efficiently, including the current lack of sustainability in the system. However, such centralization of data processing in an outsourced framework should be properly evaluated so as not to risk privacy and safety of patients. The Berlin International Working Group on Data Protection in Telecommunications has examined privacy and data protection issues in cloud computing and emphasized that cloud computing must not lead to a lowering of data protection standards as compared to conventional data processing.[77] Having a tool that will assist healthcare providers (data controller) in evaluating privacy and ethical risks before deploying e-health applications in the cloud will help in no small measures in maintaining privacy even in the cloud.

[77] The International Working Group on Data Protection in Telecommunications 2012, Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum" - 51st meeting, 23-24 April 2012, Sopot (Poland).