Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2014 Proceedings

A CROSS-COUNTRY STUDY OF CLOUD COMPUTING POLICY AND REGULATION IN HEALTHCARE

Wendy Currie
Audencia, Nantes, Ecole de Management, Nantes, France, wcurrie@audencia.com

Jonathan Seddon
Audencia, Nantes, Ecole de Management, Nantes, Nantes, France, jonathanseddon1@gmail.com

Wendy Currie and Jonathan Seddon, 2014, "A CROSS-COUNTRY STUDY OF CLOUD COMPUTING POLICY AND REGULATION IN HEALTHCARE", Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel, June 9-11, 2014, ISBN 978-0-9915567-0-0
http://aisel.aisnet.org/ecis2014/proceedings/track15/7

A CROSS-COUNTRY STUDY OF CLOUD COMPUTING POLICY AND REGULATION IN HEALTHCARE

Complete Research

Currie, Wendy, Audencia, Nantes, France, wcurrie@audencia.com
Seddon, Jonathan, Audencia, Nantes, France, jonathanseddon1@gmail.com

Abstract

International health IT policy currently supports the move towards cloud computing. Governments, industry leaders and advocacy groups are keen to build confidence among health professionals to adopt cloud-based solutions in healthcare. However, the potential benefits from cloud computing need to be evaluated against the risks. This research is a comparative study on U.S and EU health professionals' views on the potential benefits and risks from cloud computing. The results from surveying healthcare organizations in the U.S and five EU countries (France, Germany, the Netherlands, Sweden and the UK) identify differences across countries in health IT policy, incentives for adoption, privacy and security, and trust in third party suppliers. Our findings show that privacy and security are important issues for healthcare organizations, yet differences exist between the U.S and across EU Member States in how these concepts are viewed. U.S laws and EU Directives on data protection are more advanced than other international regulatory systems. Our study provides insights on cross-jurisdictional approaches to personal data and privacy, regulations and rules on health data export, how countries interpret and implement different data protection regulations and rules, and the practical implementation of regulatory rules using a comparative research method.

Keywords: Cloud computing, regulation, data security, healthcare organizations, comparative research

1 Introduction

As global healthcare budgets continue to increase, along with chronic health conditions among growing ageing populations, international governments are seeking new ways to modernize and transform their healthcare systems using information and communications technology (ICT) (Currie, 2012). Cloud computing is being promoted as a potential solution to improve health service delivery, although a number of challenges need to be overcome. However, a key challenge for international governments keen to promote cloud computing in healthcare is to provide an effective legal and regulatory framework which governs trans-border (patient) data flows. As a global phenomenon with the prospect of patient (personal) data transferring across organizational, regional and even national borders, cloud computing is developing in an un-harmonized regulatory and compliance framework, where uncertainty prevails among cloud clients and providers about how to interpret and apply international laws and 'Directives.' The regulatory landscape is a patchwork quilt which is developed in response to, rather than in anticipation of, technical change. A serious concern for policy-makers is patient data privacy and security (Movius and Krup, 2009; Mohamed, 2011) particularly as public healthcare professionals are increasingly considering private sector provisioning for the control and processing of patient data (Seddon and Currie, 2013). While

international governments continue to promote cloud computing, they are also developing new legal and regulatory reforms for the governance and protection of personal (patient) data. Healthcare organizations now face serious sanctions and penalties for data breaches, which may slow the pace of cloud computing. For healthcare, these concerns are amplified as health data is perhaps the most personal of all types of data, so attention to privacy and security issues are critical (Lohr et al, 2010; Ryan, 2010). While much of the academic literature has focused on the business case for cloud computing (Marston et al, 2011) with fewer studies linking cloud computing and healthcare (Sultan, 2014) the motivation behind this study is to provide a cross-national comparison of the intersection between cloud policy-making and adoption in healthcare organizations. This issue is becoming increasingly important to policy-makers, academics and healthcare and IT professionals, as transborder data flows are subject to different international, national and regional legal and regulatory jurisdictions. Comparative country studies therefore offer unique insights to those interested in understanding how cloud computing and other ICT policy reforms may lead to improvements or otherwise in healthcare (Papanicolas et al, 2013).

This paper adopts a comparative research method (Ragin and Rubinson, 2009) to survey six countries on cloud computing in healthcare. It responds to suggestions from academics and policy-makers which call for more cross-national studies on single health policy and ICT issues (Oderkirk et al, 2013; Seddon and Currie, 2013). While single site or case study work may provide a rich picture of ICT adoption and implementation, the results are unlikely to be generalizable outside the research setting. Equally, a cross-national study may not resolve these methodological and empirical issues. Yet it may illustrate significant differences in policy-making on health and ICT which avoids the tendency to produce 'one-size-fits-all' explanations on how a phenomenon such as cloud computing is rolled out across different healthcare environments. Further, a multi-country study on cloud policy at the national and supra-national level will provide policy-makers with a more nuanced and contextualized agenda for decision-making than a single-country analysis. It also offers the academic community some insights into the interpretation and application of health policy and ICT. This paper is divided as follows. First we consider the U.S and European regulation and compliance policy for cloud computing. We note that significant variations exist in the two approaches and further complexity arises when considering policy at the level of the nation state. Second we introduce our methods. A survey questionnaire was sent to six countries to elicit responses from health organizations on the benefits and risks of cloud computing. Third we present our results. We note that privacy and security were the most important issues for health organizations in cloud computing. However, significant differences exist in health IT policy between the geo-political regions of the U.S and EU, and also between country, state and local levels. Finally, we discuss our findings in relation to the broader international U.S and EU policy agenda for regulation of personal data in the cloud. We suggest some future directions for academic research.

2 U.S. and EU Policy on Health Data Regulation and Compliance

A key challenge for international governments keen to promote cloud computing in healthcare is to provide an effective legal and regulatory framework which governs trans-border (patient) data flows. This section gives an overview of U.S and EU policy on health data regulation and compliance. The motivation for comparing the two economic regions is twofold. First, cloud computing as a concept and practice suggests that personal, *or patient*, data is likely to be held on servers which may be located in legal and regulatory jurisdictions outside the country where the data is collected and used (Kunar, 2011). Hospitals, for example, may decide to enter into an outsourcing contract with a third party supplier to 'control' and/or 'process' their health data, which may consist of many thousands of electronic health records (EHRs) (Bell and Thornton, 2011). So cloud computing needs to be understood in a local, regional, national and cross-national context. Second, government agencies and advocacy groups (e.g. World Health Organization, OECD, World Bank) engaged in policy-making on health data regulation and

compliance are increasingly aware of the need for harmonization. This is because regulations, laws and rules that govern trans-border data flows, are developed at the country level, but are challenged at regional level (e.g. state and local conditions) and at the supra-national level (e.g. EU Directives) (European Commission, 2012ab). A lack of harmonization therefore leads to increased complexity and confusion as those who provide and procure cloud services for healthcare infrastructure and applications need to become familiar with an array of regulatory and compliance rules to avoid potential sanctions and penalties for data breaches.

The U.S government regulation for the protection of health data is enshrined in the Health Insurance Portability and Accountability Act (HIPAA) (HIPAA, 2013). The act covers a privacy and security rule. The HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities" (e.g. health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers). By regulation, the Department of Health and Human Services (DHSS) extended HIPAA to independent contractors of covered entities, defined as "Business Associates" (DHSS, 2012). PHI is any information held by a covered entity which concerns health status, provision of health care, or payment for health care that can be linked to an individual. This broad interpretation includes any part of an individual's medical record or payment history. One of the challenges for U.S. cloud providers is reassuring cloud clients that the PATRIOT Act, which extends the U.S. government's ability to access data as part of intelligence gathering activities, does not pose a risk that their data will be given to the U.S. government (Berry and Reisman, 2012). A key question is whether concerns about the PATRIOT Act influence the decisions of potential cloud customers who are reluctant to enter into cloud contracts where data centers are located outside EU jurisdictions. Multilateral agreements through directives, laws and rules govern the 28 Members States of the EU. Other countries outside this region are also looking to enter into multilateral or bilateral agreements to spearhead their own development in cloud computing.

The European Union has the Data Protection Directive (95/46). This regulates the processing of personal data across 28 Member States. It is an important part of EU privacy and human rights law (European Commission, 2013). Data protection is enshrined in the Treaty on the functioning of the EU where personal data protection is the right of all citizens. The Directive was adopted to harmonize national provisions on the protection of individuals in the processing and free movement of personal data. In 2010, a communication adopted by the European Commission discussed the new challenges for personal data protection in the context of cross-border data flows. In 2012, a draft European General Data Protection Regulation was unveiled to supersede the Data Protection Directive. The comprehensive revision of the Directive was launched to address key aspects of processing personal health data, to ensure privacy for patients, and to enable the EU to meet the other legitimate objectives in the Treaties, including more robust health data protection. An EU company may transfer, or make accessible, personal data to a company outside the EU only if an "adequate level" of data protection is ensured by the recipient. An adequate level of data protection is further applied to intra-group transfers (e.g. if the Data Exporter and Data Importer belong to the same group of companies). The EU Directive claims that a data transfer happens if the Data Importer has access to personal data of entities established in the EU. An example is access to servers controlled by EU subsidiaries. A Data Exporter and Data Importer may sign a contract that includes the EU standard contractual clauses where the latter offers an adequate level of data protection. The Directive requires EU Member States to adopt relevant national legislation. So far, Member States adopt varying approaches to the formal requirements and obligations. Some EU jurisdictions have adopted the standard contractual clauses, with others imposing more stringent requirements for the use of the clauses. Currently, over sixty countries in all world regions have adopted data protection and privacy laws that regulate transborder data flows, most of which are largely based on one or more of international and regional instruments. Initiatives are underway in many regions and countries to review national and regional approaches, and to consider whether an international instrument on data protection and privacy could be adopted (Kunar, 2011). The academic literature on cloud computing points to a series of potential challenges for policy-makers (Loebecke et al, 2012) and business

leaders (Marston et al, 2011; Venters and Whitley, 2012) in identifying the benefits and risks of this technology. Within healthcare, cloud computing is segmented by software applications, deployment models and service/pricing options (Iyer and Henderson, 2010). Healthcare applications include clinical information systems (CIS) and non-clinical information systems (NCIS). Other systems used in healthcare which may not be described using the term 'cloud' may involve health information exchanges (HIEs), electronic patient records (EPRs) and mobile health or mHealth devices and applications.

Across the healthcare industry, four deployment models include: private, public, hybrid and community clouds. Service models in the cloud market are classified into Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Network-as-a-Service (NaaS) and Infrastructure-as-a-Service (IaaS). The public cloud services market is forecast to grow 18.5 percent in 2013 to total $131 billion worldwide, up from $111 billion in 2012. The IaaS market is the fastest growing segment, growing 42.4 percent in 2012 to $6.1 billion and expected to grow 47.3 percent in 2013 to $9 billion (Gartner, 2013). Cloud delivery may therefore take the form of one-to-one, one-to-many or many-to-one, where health data (clinical or administrative) passes through a cloud network. A compelling motivation for Cloud computing is the promise of reducing the total cost of ownership (TCO) of software, hardware and services for public healthcare organizations looking to reduce cost. Based on a utility, pay-per-use service model, cloud vendors offer two types of pricing models: pay-as-you-go or a subscription-based/spot pricing model (Huang and Dan, 2013) which may enhance business value to users (Iyer and Henderson, 2012). Within the healthcare environment, personal or patient data is highly sensitive and valuable to both research institutions and commercial organizations (Seddon and Currie, 2013). Policy-makers are keen to promote cloud computing, recognizing that health data regulation and compliance in the U.S and EU will need to be adapted for different regional and local environments (Mell and Grance, 2011). While this approach may provide general policy guidance, European countries all have their own health and eHealth policy (European Commission, 2012ab). This suggests that while the EU is a relevant entity for examining supra-national policy, the level of analysis should also include the country, or *nation state* as this will impact on other levels and units of analyses including healthcare organizations and professional practices.

3 Methods

Within the information systems literature, cross-country studies on ICT in healthcare are relatively scarce. In particular, there are few studies which use quantitative metrics or indicators to compare and contrast health and ICT for guiding policy- making (Papanicolas et al, 2013). Methodological challenges exist in collecting data from more than one country, and it is essential that concepts need to 'travel' or be relevant across geographical, economic and cultural environments. The emergence of cloud computing, however, offers an opportunity and a challenge for IS researchers. Cloud computing is not simply an 'IT challenge' for the business community, since it needs to be understood in the context of the legal and regulatory framework which governs potential trans-border data flows. As we discussed above, this is an important policy issue for U.S. and EU policy-makers, regulators and industry leaders, especially in terms of protecting personal (patient) data. Numerous reports and commentaries exist from the IT industry emphasizing the benefits from cloud computing. There are many 'white papers' from legal firms attempting to sell their expertise to healthcare organizations (and other industries) for entering into outsourcing deals with cloud providers. Against a background of this material, we developed a questionnaire survey to elicit responses from healthcare organizations currently using or planning to use cloud computing for various clinical and non-clinical reasons. The survey instrument comprised many questions relating to the type of healthcare organization, the range of cloud-based applications, incentives and dis-incentives for adopting, policies on patient data sharing, and integration of cloud-based infrastructure and applications. Due to space limitations, this paper will include only the results from the incentives and dis-incentives to use cloud computing.

Europe represents a very diverse collection of economies. Populations vary from over 82m in Germany to just over 0.5m in Luxembourg. Belgium, with 11.8% has the highest total health expenditure as a percentage of GDP, whilst Romania with 5.4% has the lowest. And Finland with 100% has the highest use of computers during consultation whilst at 2.8% Latvia has the lowest. Based on our extensive literature review (which we are unable to include in this paper), the focus was given to those countries which were considered more advanced in implementing and using cloud services, combined with an established ICT infrastructure and growing economies. The five European countries selected for this survey were: France; Germany; Netherlands; Sweden and the UK. While France, Germany and the UK, all have large populations, with the Netherlands fourth highest, Sweden is a relatively small country, yet is often seen as among the front-runners in eHealth (Currie, 2012). These countries all have mature healthcare systems, yet demonstrate some variation in their legal and regulatory approach to cloud computing, particularly in data protection and privacy. Unlike countries, largely in Eastern Europe, which have lower developed healthcare systems, these five EU Member States were selected as offering potentially large markets and/or maturity for developing cloud computing in healthcare. We further selected the United States for comparison with the EU countries. Firstly, the U.S, with over fifty states offers a large economic region which is undergoing considerable change in terms of its healthcare provisioning. Second, it represents a world leader in developing cloud-based solutions, for healthcare and other industries. Yet is also has a different legal and regulatory framework, not only in comparison with the E.U, but also across federal and state lines, and even within states. While this study is unable to capture all these differences, it is important to recognize that, for comparative purposes, cloud provisioning in healthcare is potentially deployed under many different regulatory and compliance jurisdictions. The choice of countries was agreed with our main sponsor, Microsoft, who provided access to experts in cloud computing policy and regulation, government affairs, technology architecture, privacy/security and representatives of patients groups. The U.S-EU comparison was seen as particularly relevant for policy-makers, industry leaders and academics many of whom adopt an ethnocentric approach to both healthcare and cloud computing. A professional survey firm was used to identify and administer the questionnaire survey. All questionnaires were translated into the language of the country by native speakers. A total of 2085 questionnaires were sent using the Internet to the six countries. 553 were returned (fully usable) which is a 27% response rate. Table 1 gives a breakdown of the responses for each country, as a percentage of type of health service, and the roles within these services. The numbers in brackets showed how many questionnaires were used from each country. These questionnaires were sent to healthcare organizations only. They include: clinics; general practice; hospitals and nursing homes. Respondents are categorised into six health professional groups: administration; carer; IT; medical; nurse and research.

Table 1. Healthcare Organizations in six countries

		DEU (108)	**ENG (99)**	**FRA (98)**	**NLD (46)**	**SWE (102)**	**U.S (99)**
Type of Health Service	Clinic	10	6	14	13	5	13
	General Practice	20	15	15	2	46	25
	Hospital	40	57	57	35	19	47
	Nursing Home	30	22	14	50	30	15
Respondent's role	Administration	15	10	22	13	14	22
	Carer	24	9	20	37	37	14
	Information Technology	5	15	5	9	3	6
	Medical	17	49	25	17	14	31
	Nurse	35	2	24	20	28	23
	Research	4	15	4	4	4	4

The survey questions were derived from an extensive literature review of ICT policy and regulation at the U.S and EU levels, cloud computing literature (academic and business) and the health IT literature. The questionnaire was validated by the sponsor organization, and by professional and academic reviewers. To comply with comparative methodologies for conducting both quantitative and qualitative research (Pennings et al, 2006) it is essential that survey questions are transferable and easily understood by potential respondents. The researchers' definition of Cloud Computing was presented to each questionnaire respondent: *"Cloud based services can be thought of as programs that are accessed via the Internet. Data is stored remotely rather than on the device that is being used".* The first question asked was "*Do you use the internet to store, process and communicate information*". If the answer was either *'No'* or *'Don't know'* then the questionnaire was terminated. All of the responses presented in this paper are from respondents who answered either *'Yes'* or *'Plan to'*. Since the survey included a wide range of countries, it was important to retain a simple approach to the meaning of cloud computing, since this was translated into the language of a given country. We were not interested in this survey to elicit responses on the many different types of cloud offerings, as we were informed by the survey company that 'less is more' in terms of receiving usable returned questionnaires. Thus our main interest was to gain an understanding and appreciation of some of the identifiable differences across the six countries, which did not extend to, with this survey instrument, variation across state and local levels. While the survey contained several questions, our space limitations mean that we are only able to present the findings from a limited dataset.

4 Results

In the next section we will present the findings from just two of the survey questions: *1) Please evaluate the following benefits from 'Cloud' computing, 2) Please evaluate the risks from 'Cloud' computing*

The aggregated results for the first question are given in Table 2, and those for the second in Table 3. Looking at Table 2, the averaged percentage scores for each of the five European countries used in the survey are shown, together with the U.S. results. For the five European countries, the highest score for all of these questions was 'Very important' with the exception of 'Access data anywhere/ anytime/ anyplace' where it tied with 'Extremely important'. The U.S. answered each question as being 'Extremely important' – apart from 'Improve decisions via improved data sharing' which was regarded as 'Very Important'. The concept of Cloud technology is more developed and established in the U.S. Not only for the applications that are developed, but also for supporting mobile and internet based tools that are required. As the U.S is introducing a national policy to introduce EHRs, the response of 'Extremely important' may reflect this generic policy, unlike the more measured approach of the EU, while having a pan-European policy on cloud, still maintains a fragmented and diverse approach at Member State level.

In this paper, further analysis of this data was done by considering only the 'Extremely important' responses. From the underlying data used to for the European averages, the standard deviations (SD) vary from 5.2 (Improve decisions via improved data sharing) to 8.3 (Increased efficiency in data collection and retrieval). Given that the U.S scores are higher for every indicator, it is not surprising that the revised SD calculations when including these scores all increase from between 20.2% (Improvement in quality of service) to 39.2% (Increased efficiency in data collection and retrieval). Figure 1 presents this underlying data, together with the European average, ordered by the U.S. score. The data points for both the U.S and EU average are indicated by blocks to improve readability. The U.S. and EU lines show that both are trending in the same direction, but the U.S. regard these benefits as being higher for every question asked. Looking at the EU countries, England scores the highest on four of the questions, Germany on two and France and the Netherlands on one. The closest EU and U.S. scores were for 'Access data anywhere/anytime/anyplace', where the UK was just over 8% lower. The greatest difference between

these scores was for the question asking about the benefits for 'Services to be easily deployed'. Here, the Swedish score was almost 72% lower than that from the U.S.

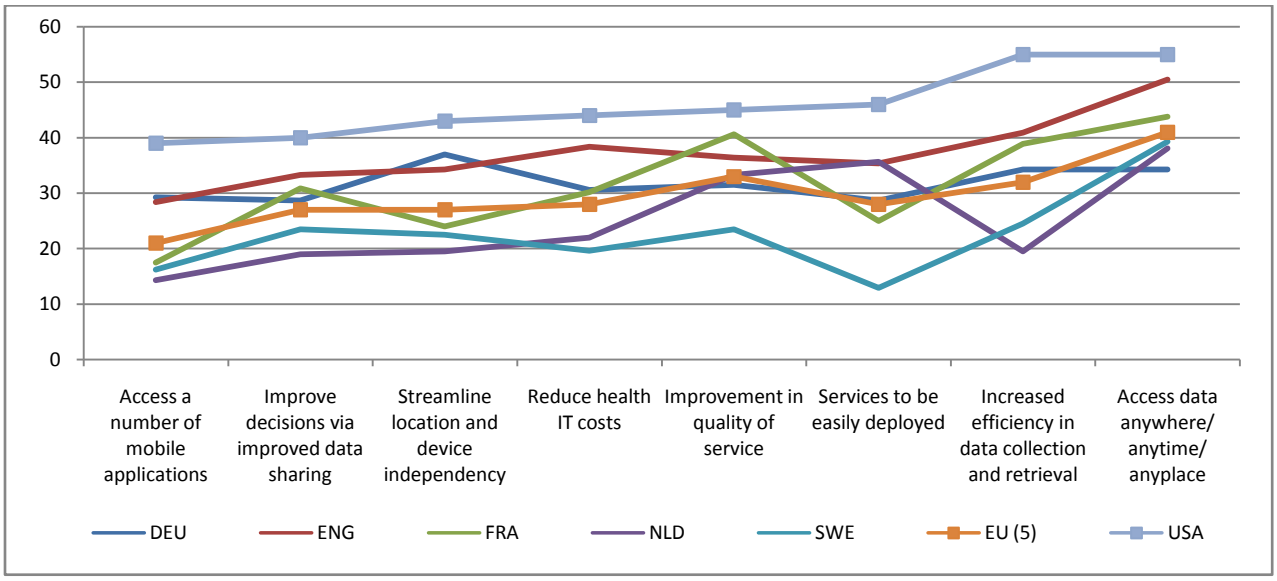
Table 2. Average European and U.S Responses to Cloud Benefits

		Access a number of mobile applications	Improve decisions via improved data sharing	Streamline location and device independency	Reduce health IT costs	Improvement in quality of service	Services to be easily deployed	Increased efficiency in data collection and retrieval	Access data anywhere/ anytime/ anyplace
EU	**Not at all important**	10	4	4	5	4	4	3	5
	Slightly important	26	18	21	17	11	17	12	13
	Very important	43	51	48	50	52	52	53	41
	Extremely important	21	27	27	28	33	28	32	41
U.S	**Not at all important**	6	5	6	2	2	3	5	4
	Slightly important	23	13	14	12	15	8	9	12
	Very important	32	42	36	41	37	42	31	29
	Extremely important	39	40	43	44	45	46	55	55

Please note that due to rounding issues country scores may not add up to 100

Figure 1 shows the tightest spread amongst the European responses is for 'Improve decisions via improved data sharing', where 14% separates the maximum England and minimum scores for the Netherlands. This English score is still 17% less than the U.S's score. The second tightest EU spread was for 'Access a number of mobile applications'. Here just 15% separated the German score from the Netherlands, and this is 10% less that the U.S. score. The question asking whether cloud benefits 'Services to be easily deployed' had the largest spread, with England's 35% being 22% higher than that for Sweden. The U.S. value of 46% was this country's third highest score. One other question that had a large EU country spread was for 'Increased efficiency in data collection and retrieval'. Here, 21% separated the Netherlands score of 20% and the English score of 41%, yet still 14% behind the U.S score of 55%. Looking at the EU countries, England has a consistently high score. This was perhaps related to almost 50% of the respondents identifying themselves as 'Medical' staff. Sweden and the Netherlands are the most conservative over the benefits that cloud computing offers. Reasons why the Netherlands results are low, given its relative strong progress in eHealth (European Union, 2012ab) could be due to its low number of respondents and a skew due to 37% of the respondents being a 'Carer'. Interestingly looking at Table 1, the role percentage for Sweden closely matched that of the Netherlands, despite having more than twice as many respondents.

Figure 1. European and U.S score for 'Extremely important' cloud benefits



Respondents across the six countries were also surveyed for their views on the risks from cloud computing. The aggregated results for this question are presented in Table 3. This table shows the averaged percentage scores from each of the five European countries, together with the U.S. score. By far the most serious risk is in the area of privacy and security of clinical data. This risk was considered by 63% of EU respondents as 'extremely important' and reflects the serious challenges facing EU policy-makers, health professionals and the IT industry in developing effective ways to protect patient data. Similarly, 71% of U.S respondents said this risk was 'extremely important. Given that cloud computing is more established in the U.S. it is illuminating that they have the highest concern about this risk. The highest scores for both the U.S and Europe are for the questions answered 'Very important'. Given the survey results generated Table 2 focused on the 'Extremely important', it was decided to also use this response for the data in Table 3. It is interesting to note that the combined totals for the 'Very' and 'Extremely' important questions are almost the same for each question for Europe and the U.S. Figure 2 presents this underlying data, together with the values for the average of the European countries. This graph has been ordered by the US score, with its data points and those for the EU indicated by blocks to improve readability. The 'spike' at the tail of this graph reflects how every country has similar concerns about the privacy and security of clinical data.

Whilst the US has a score of 71%, Germany and England scored 69%. For this question, all of the EU and U.S. scores are much closer together than they were in Figure 1. The US no longer dominates the graph for the highest scores, and with the exception of 'Trust in 3rd party provider', the SD for all of these answers is much closer that those used to generate Table 2. They vary from 3.3 for 'Data is used for commercial purposes' up to 6.3 for 'Privacy and security of clinical data'. The highest value of 11.6 is for 'Trust in 3rd party provider' because of a very low score from the Netherlands. If this value is removed, the standard deviation drops to 6.6. France has the highest scores for two of the measures (Poor incentives for adoption and General resistance to change), Sweden one (Data is used for commercial purposes) and the US for all of the rest. The second most important risk was 'trust in 3rd party provider'. This did not appear to be a serious risk for respondents from the Netherlands, yet for all other EU countries, it was either on or above the EU average score, with Germany, closely followed by Sweden, identifying this risk as 'extremely important'. A surprising result was that only France scored above average for 'Poor incentives for adoption' for cloud computing. France has one of the most mature and well-funded health

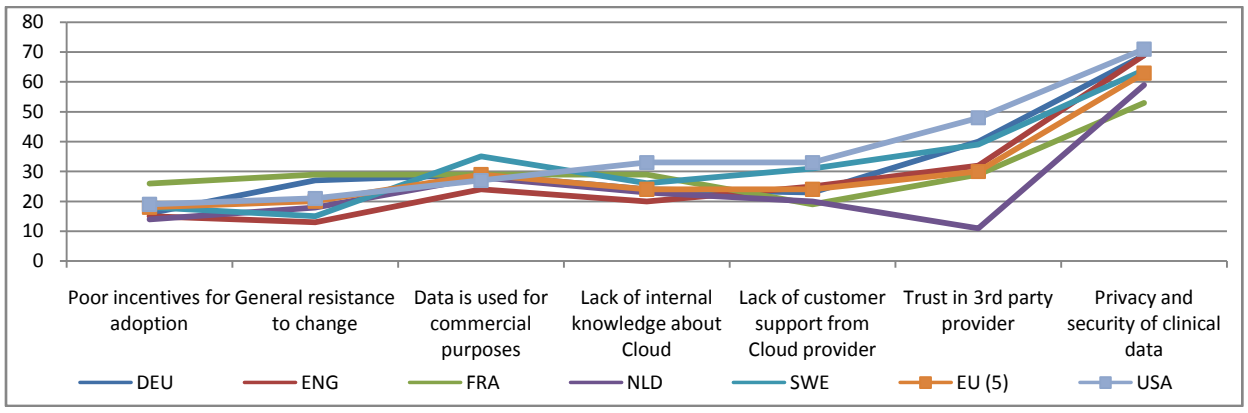
systems of all EU countries. Incentives systems for health professionals to adopt cloud computing are therefore more likely to become an obstacle in policy-making to promote cloud computing in health systems which are working well, unlike in other countries which are trying to improve their health services.

Table 3. Average European and U.S Responses to Cloud Risks

		Poor incentives for adoption	General resistance to change	Data is used for commercial purposes	Lack of internal knowledge about Cloud	Lack of customer support from Cloud provider	Trust in 3rd party provider	Privacy and security of clinical data
EU	Not at all important	11	12	14	8	7	5	2
	Slightly important	31	23	21	20	23	20	5
	Very important	40	45	36	48	46	45	30
	Extremely important	18	20	29	24	24	30	63
U.S	Not at all important	13	11	7	6	7	4	3
	Slightly important	29	27	26	26	19	16	6
	Very important	38	40	39	34	41	32	20
	Extremely important	19	21	27	33	33	48	71

Please note that due to rounding issues country scores may not add up to 100

Figure 2. European and U.S score for 'Extremely important' cloud risks



5 Discussion

Cloud computing is a growing phenomenon which is yet to reach its potential in healthcare as in other industry sectors (Berry and Reisman, 2012). While it is technically well developed, our comparative survey of six countries with mature health systems suggests that health professionals recognize the potential benefits from cloud computing, but also see potential pitfalls. While incentives to change U.S and EU healthcare systems are driven by the rising cost of healthcare, ageing populations, growth in

chronic (long term) conditions, increased patient demands for improved health services, etc, cloud computing is attractive to policy-makers since it offers increased opportunities to modernize health service delivery (Currie, 2012). The policy direction to encourage citizens to participate in their healthcare (e.g. patient centric care) is designed to transform health services to enable more home care, flexible diagnosis, monitoring and treatment of health conditions (e.g. treating the elderly in their own home using remote devices). However, these challenges are not only economic and social, but also cultural and political. Changing health systems to incentivize patients to become 'actively engaged' in their health and wellbeing is a cultural shift from the traditional approach where health professionals diagnose and treat 'passive' patients, who rarely question medical opinion (European Commission, 2012ab). The medical profession also need to be incentivised to adopt new technology, particularly where doctors are paid to treat patients on a 'fee for service' model, which is different from self-provisioning patients who access information and advice over the Internet.

Our comparative survey of cloud computing across six countries, all with mature health systems suggests that health professionals are generally in favour of adopting cloud computing, with the U.S seemingly more vocal about the range of benefits seen as 'extremely important' compared with most EU countries. However, policy-makers need to provide further incentives to engage health professionals. While U.S and EU politicians are heavily promoting eHealth through a range of policies to support industry and research, particularly job creation schemes (Jaegar et al, 2008) our results indicate that by far the most serious risk is defining and implementing a legal and regulatory framework to protect health data. Regulation and compliance for cloud computing is a fast-moving field which follows rather than precedes technical change (Ward and Sipior, 2010). Within the academic literature, discussion on regulation and compliance in healthcare is largely found in the legal field rather than in the IS community. Yet the scale and scope of health regulation is now becoming a serious issue, not just for the policy-makers who are keen to protect citizens from issues, such as data breaches, but also for health professionals and IT companies who seek to change health service delivery using cloud computing, and other technological artefacts. Currently, U.S and EU data protection for cloud computing in healthcare reveals a complex mix of mandatory and voluntary influences on cloud stakeholders. Regulation attempts to ensure that cloud clients and providers guarantee adequate protection of citizens' data (Kunar, 2011). The literature sources point to some interesting observations, but need to be understood and interpreted for their own geo-political or regional area. In the U.S. the HIPAA regulations provide citizens with some assurances that healthcare organizations entering into outsourcing contracts with cloud providers will need to ensure that health (clinical) data is governed according to a stringent set of rules to ensure full compliance (Schweitzer, 2013). Healthcare organizations will need to be careful to avoid entering into contracts with cloud providers who do not comply with HIPAA privacy and security rules. Penalties for non-compliance will extend to the data controller and data processor, which include the client organization (e.g. healthcare provider) cloud provider, and also possibly the sub-contractors hired by the primary contractor. The EU region is more complex, given there are 28 EU Member States, all with their own governments and data protection laws and policies. The EU Directive has helped to professionalize and harmonize data protection across Europe, although implementation within and outside the region varies (Robinson et al, 2009). Continuing with a unilateral approach to data protection laws executed by individual EU member states is less viable in a global market for cloud computing. But even a pan-European Directive on data protection, incorporating the EEA countries, will be a challenge. Cloud providers offering a diverse range of services (e.g. SaaS, PaaS, IaaS, NaaS) in and outside the EU region will present serious challenges to any regulator to fully monitor national and trans-border data flows. This applies to healthcare as well as other industries.

Secondly, the complex array of existing and proposed regulation imposes additional burdens on cloud clients and providers. Understanding the terminology of 'controllers', 'processors' and sub-processors', in addition to delineating the various roles and responsibilities of these different groups extends beyond an organizational and managerial agenda to become a legal matter. Failure to adequately understand and

execute these roles internally and externally is likely to increase risk, particularly where financial sanctions are imposed for serious data protection infringements. Our six country study showed that while health organizations largely perceived cloud computing to offer 'extremely important' benefits in terms of accessing patient data 'anytime, anyplace, anywhere', this was balanced by serious concerns about potential privacy and security threats. So if international governments are to build capacity for the digital economy, the right balance is needed between developing viable and effective regulatory controls with providing the freedom and support to promote 'cloud readiness' (Loebecke et al, 2012). Currently, the cloud market is infused with mixed political and economic messages, where companies and citizens are encouraged to adopt cloud computing, yet at the same time, are made aware of their responsibilities for infringing the personal data of individuals through poor privacy and security controls (Owens (2009). The stringent U.S. HIPAA privacy and security rules encourage people to report data infringements to the government regulator, where fines and penalties if found guilty are very severe. Such a move is likely to slow the market for cloud computing, and especially in healthcare organizations where ICT capability may be low.

Our findings suggest that for many health organizations, cloud computing is a new phenomenon where the learning curve for understanding and evaluating cloud benefits and risks is not helped by the many conflicting and contradictory messages from governments, industry and other interested parties who promote this emerging technology. Healthcare organizations working with third party cloud providers will need to become familiar with the diverse regulatory controls, both inside and outside U.S and EU jurisdictions. This will become even more important with the shift away from self-regulation towards mandatory controls and sanctions for non-compliance (Mell and Grance, 2011). As our aggregate data suggested, trust in a third party cloud provider was perceived as an extremely important risk factor for all countries, barring the Netherlands. Health organizations which store highly sensitive patient data will need to develop additional legal, business and technical capabilities to be able to negotiate with cloud providers. In particular, they will need to gain a deep knowledge of the roles of controller, processor and sub-processor in terms of accountability and risk. Signing the cloud provider's SLA will not be sufficient, without first having undertaken a full risk assessment of how patient data will be controlled and processed. While the EU Directive is a reference model for good practice, with standard contractual clauses, the current cloud market offers a diverse range of services, with varying levels of privacy and security protection. Potential healthcare cloud clients need to ensure they are fully aware of these issues as the cloud providers are unlikely to volunteer information on the entities involved in managing personal data within a multi-contract cloud outsourcing agreement. Ensuring an adequate level of data protection is an essential compliance requirement for companies in the EU, although wide variations exist in national laws in regard to privacy and security. In Germany, for example, infringement of the strict data protections laws can result in administrative fines of up to €300,000. Under German law, companies are obliged to appoint an in-house data protection officer with direct reporting responsibilities to senior management. This individual oversees the company's compliance requirements which include evaluating whether a data processor outside the EU can guarantee an adequate level of data protection. Our survey results showed that German health organizations were equally as concerned as the U.S respondents about privacy and security risks. These similarities need to be further researched as different national laws, professional practices and potential sanctions, are just some examples where the two countries may differ.

The study had a number of limitations. Firstly, our comparative research approach was only made viable by recognizing that research questions targeted at different countries need to be simple and straightforward (Ragin and Rubinson, 2009). The aim of this study was not to provide in-depth country analysis of cloud computing, but instead to elicit responses from cloud users across healthcare organizations in six countries with mature health systems. The responses to our questions, while providing a snapshot of respondents' views about potential benefits and risks from cloud computing, needs to be supplemented by additional cross-country research, possibly on a single issue such as data privacy and security. Second, our questionnaire was relatively modest, where we sought around 100

usable responses. Usable questionnaire from the Netherlands provided a small sample size of forty-six, thus reducing the representation for this country. Similarly, relatively few responses from specific healthcare organizations, such as 6% came from English clinics, again makes it difficult to provide comparative analysis at the organizational level of analysis. Further research may therefore place more attention on the types of health organizations and their respective policies and plans for cloud computing, as opposed to this study which discusses the results of the various healthcare organizations under this single heading. Future studies may therefore select a specific type of health organization, e.g. general practice, and compare and contrast the findings at an international, national or regional level. Thirdly, the risk of 'social acceptability' needs to be addressed. This is where the respondent, or 'end user' in the case of cloud computing, may respond in a way that is believed to have been desirable, given their particular role or responsibility. It is evident from international government policy in the U.S. and across the EU that cloud computing is being promoted for a range of socio-political and economic reasons. In the U.S eHealth is promoted with a range of incentives for adoption by clinicians (HIPAA, 2013). While it is outside the scope of this study to rehearse these issues, it is likely that the 'technology push' for cloud computing will lead to some bias in the responses received. However, this situation is likely to afflict all questionnaire survey research as responses are always given within a particular political and cultural milieu. Finally, respondents were given four options for answering questions, rather than five. This was based on advice given, since respondents are more likely to gravitate to 'average importance' in questionnaires rather than choosing a more definitive option, e.g. 'extremely important', 'very important', 'slightly important', 'not at all important'. The limitation is in the lack of granularity in the responses given.

6 Conclusion

This study offers three conclusions and recommendations for future research. Firstly, our review of the policy and academic literature supports more comparative research in information systems where the IT artefact, such as cloud computing, potentially has cross-jurisdictional implications for policy-makers, regulators, IT industry and cloud clients. Our focus on healthcare organizations in six countries, characterised by very different political, social and economic systems suggests that cloud computing within healthcare needs to be understood in a wider disciplinary context. The potential growth in cross-jurisdictional health data transfers using cloud computing raises issues about how to protect the personal data of citizens. Our aggregate country data suggests that cloud computing is currently being used across health organizations, albeit with serious concerns about privacy and security. So far, international governments are falling behind the rapid pace of technical change, as they rush to pass new Directives, laws and rules to ensure that all parties protection the privacy and security of citizens' personal data (Ward and Sipior, 2010). Secondly, this study has implications for outsourcing research within the IS field (Chow et al, 2009). Our country data suggests that healthcare organizations are concerned about working with third party providers in relation to cloud computing. While this may be a trust issue, it may also stem from concerns about how to develop and execute a sufficiently robust cloud computing contract. Linking our findings to existing literature, it seems that cloud clients (e.g. health organizations) are likely to enter into standard contractual clauses with cloud providers, which may not fully protect the rights of all parties, including the individuals whose personal data is being stored (Seddon and Currie, 2013). Governments and industry advisors advise cloud clients about the need to read the small print of these contracts rather than treating them as just an administrative formality (Buttarelli, 2012). However, within public health across the U.S and Europe, it is unlikely that sufficient expertise exists. As cloud computing is a relatively new phenomenon, unlike previous technology which resides within a single organization, it has the potential for trans-border data flows across multiple legal and regulatory jurisdictions. All cloud stakeholders therefore need to work their way through what is currently a complex array of legal and regulatory issues. Thirdly, this study shows that cloud computing extends beyond the

technical remit to include broader issues in international public and health policy, where cloud computing becomes part of a wider information policy (Jaeger et al, 2008). As the U.S government and EU play a part in designing (often complex) regulation and compliance mechanisms, greater transparency and accountability is needed, particularly as terms such as controllers, processors and sub-processors are not widely recognized by healthcare organizations and citizens more generally (European Commission, 2012b).

This study has several limitations, not least because it provides only a snapshot of cloud computing benefits and risks across six countries from a relatively diverse range of healthcare organizations. In this paper, we can only report a limited dataset due to space limitations. While cross-national studies are in demand from policy-makers and by some academic communities, it is important that conclusions are not drawn from the data which intentionally or unwittingly results in false comparisons. In this study, we suggest that while cloud computing is an interesting phenomenon which is being pursued by U.S and EU governments, the underlying policy direction needs to be understood. This is made more complex as the U.S has different federal and state laws governing cloud computing, including data security and privacy as does the E.U. with its complex mix of 28 Member States. It is therefore important to gain an appreciation of the health ICT policy environment as a backdrop for interpreting the results from either quantitative or qualitative research. Another limitation is that our generic survey does not provide details of the different types of cloud infrastructure and applications used across the sample organizations. Healthcare uses a wide mix of technologies which may extend beyond ICTs, including medical devices, monitoring equipment and even medicines. All may be referred to as ‘health technologies’ (Currie, 2012). While our extended survey includes some questions on cloud offerings in healthcare, the blurring of technical boundaries, particularly in terms of patient data which may be held on many devices (e.g. PCs, mobile phones, servers) where it travels across different jurisdictions (e.g. within and across countries) is also a potential limitation. This research is not focused on the healthcare ICT artefact at the site or company level. Instead, it adopts a top-down approach on the intersection between cloud policy and cross-country comparisons, as this was required by our sponsors, many of whom did not wish to see yet more academic studies on cloud computing adoption and implementation using a single cloud application and/or in one country or organization. Despite the limitations of this study which extends to cross-national comparisons more generally, our findings offer some value to those interested in gaining a more nuanced understanding of how health ICT policy at the national level impacts on the diffusion of an emerging technology (e.g. cloud computing) both across and within national jurisdictions. Paradoxically, while governments are keen to promote cloud computing, their concerns about patient data breaches among other potential threats force them to develop increasingly punitive regulatory and compliance systems which inhibit or slow market development. Further research may therefore explore this relationship, or tension, at the societal level. Additional work may focus on the adoption of specific cloud-based offerings within healthcare organizations, but link the findings to the macro level. From our limited set of findings, the area of privacy and security in the cloud remains an important topic for further research, yet this needs to take into consideration, not simply the relationship between data controllers and processors (Seddon and Currie, 2013) but also how potential violations fall under the scrutiny of different regulatory bodies which are facing an increasing struggle to keep pace with technological change.

References

Bell, B, Thornton, K. (2011). From promise to reality achieving the value of an EHR. Healthcare Financial Management, 65(2), 51-56.

Berry, R. and Reisman, M. (2012) 'Policy challenges of cross-border cloud computing'. Journal of International Commerce and Economics.

Buttarelli, G (2012) 'Security and privacy regulatory challenges in the Cloud'. Speech by European Data Protection Supervisor. www.Edps.europa.eu. 21 March, Brussels.

Carroll, J.M. (1974) The problem of Transnational Data Flows', in Policy Issues in Data Protection and Privacy, Proceedings of the OECD Seminar 24 to 26 June, 1974, p.201.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., Molina, J. (2009) 'Controlling data in the Cloud: Outsourcing computation without outsourcing control'. CCSW'09.November 13, Chicago, Illinois, U.S. ACM 978-1-60558-784-4/09/11.

Currie, W.L. (2012). TEMPEST: An integrative model of health technology assessment. Health Policy and Technology, 1:1, 35-49.

Doering, N., Legido-Quigley, H., Glinos, I.A., Maarse, H. (2013) A success story in cross-border telemedicine in Europe: The use of intra-operative tele-neuromonitoring during aorta surgery. Health Policy and Technology, 2:1, 4-9.

European Commission (1995) Directive 95/46/EC of the European Parliament and the Council. Official Journal of the European Communities, No.L 281/31.

European Commission (2012a).Article 29 Data Protection Working Party. Opinion 05/2012 on Cloud Computing. 01037/12/EN WP 196.

European Commission (2012b) Unleashing the Potential of Cloud Computing. COM (2012) 529 final.http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/swd_com_cloud.

European Commission (2013) ec.europa.eu/justice/data-protection/index_en.htm.

Foster, I., Zhao, Y., Raicu, I., Lu, S. (20080 Cloud computing and grid computing 360-degree compared. Proceedings of the IEEE GCEW, pp. 1-10.

Gartner Group (2013) Worldwide Public Cloud Services Market.http://www.gartner.com/newsroom/id/2352816.

HIPAA (2013) Federal Register on January 25, 2013. www.hipaa.com/2013/02/hipaa-final-rule-modification-of-business-associate-definition-part-3/

Huang, J., Dan, MA. (2013) The pricing model of cloud computing services. Research Collection School of Information Systems (Open Access).Paper 1742.http://ink.library.smu.edu.sg/sis_research/1742.

Iyer, B., Henderson, J.C. (2012) Business value from Clouds: Learning from Users. MISQ Executive. 11:1, 51-59.

Iyer, B., Henderson, J.C. (2010) Preparing for the future: Understanding the seven capabilities of Cloud Computing. MISQ Executive. 9:2, 117-131.

Jaeger, P.T and Lin, J., Grimes, J.M. (2008) Cloud Computing and Information Policy: Computing in a Policy Cloud? Journal of Information Technology & Politics, Vol. 5 (3), 269-283.

Kunar, C (2011) Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future.

Loebecke C., Thomas, B., Ullrich, T. (2012) Assessing cloud readiness at Continental AG.MISQ Executive. 11:1, 11-23.

Lohr, H., Sadhegi, A.R., Winandy, M (2010) 'Securing the E-Health Cloud. IHI'10. November 11-12, Arlington, Virginia, U.S.ACM 978-1-4503-0030-8/10/11.

Marston, S., Li. Z., Bandyopadhyay, S., Zhang, J., Ghalsasi, A. (2011) 'Cloud computing – The business perspective'. Decision Support Systems, 51, 176-189.

Mell, P., and Grance, T (2011) The NIST Definition of Cloud Computing. National Institute of Standards and Technology (NIST) (http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf).

Mohammed, D. (2011) Security in Cloud Computing: An Analysis of Key Drivers and Constraints. Information Security Journal: A Global Perspective, 20: 123-127.

Movius, L.B., Krup, N. (2009) U.S. and E.U. Privacy Policy: Comparison of Regulatory Approaches'. International Journal of Communication, 3, 169-187.

Oderkirk, J., Ronchi, E., Klazinga, N. (2013) "International comparisons of health system performance among OECD countries: Opportunities and data privacy protection challenges". Health Policy, 112, 9-18.

Owens, D. (2009) Securing Elasticity in the Cloud. Communications of the ACM. 53 (6) 48-51.

Papanicolas, I., Kringos, D., Klazinga, N.S., Smith, P.C. (2013) "Health System Performance Comparison: New Directions in Research and Policy". Health Policy, 112, pp. 1-3.

Pennings, P., Keman, H., Kleinnijenhuis, J (2006) Doing research in political science. Sage, UK.

Ragin, C.C., and Rubinson, C. (2009) The distinctiveness of comparative research in T.Landman and N. Robinson. The SAGE Handbook of comparative politics, Sage, UK.

Robinson, N., Graux, H., Botterman, M., Valeri, L (2009) Review of the European Data Protection Directive. Rand Europe. International Commissioner's Office.

Ryan, M. (2010) Viewpoint: Cloud computing privacy concerns on our doorstep. Communications of the ACM. 54 (1) 36-38.

Schweitzer, E.J. (2013) 'Reconciliation of the Cloud computing model with US federal electronic health record regulations'. Journal of the Medical Information Association, 19:161-165. doi:10.1136.(http://www.euractiv.com/infosociety/brussels-unveils-cloud-computing-news-515057).

Seddon, J.J.M., Currie, W.L. (2013) 'Cloud Computing and Trans-Border Health Data Flows: Unpacking US and E.U. Regulation and Compliance'. Health Policy and Technology, 2:4.

Sultan, N. (2014) 'Making use of cloud computing for healthcare and challenges'. International Journal of Information Management, 34:2, 177-184.

Venters, W., Whitley, E. (2012) 'A critical review of cloud computing: researching desires and realities'. Journal of Information Technology, 27, 179-197.

Ward, B.T and Sipior, J.C. (2010) The Internet Jurisdiction Risk of Cloud Computing. Information Systems Management, 27: 334-339.

Wolf, C and Tobin, T.P. (2007) Chapter 28: Privacy Laws. In Proskauer on International Litigation and Arbitration: Managing, Resolving, and Avoiding Cross-Border Business or Regulatory Disputes. New York: Proskauer Rose LLP.

Zhang, Q., Cheng, L., Boutaba, R. (2010) Cloud computing: State of the art and research challenges. Journal of Internet Service Applications, 1 (1) 7-18.