Association for Information Systems
AIS Electronic Library (AISeL)

MCIS 2014 Proceedings

Mediterranean Conference on Information Systems (MCIS)

Summer 9-4-2014

INSTITUTIONAL EFFECTS OF COMPARATIVE GOVERNMENT REGULATION FOR THE PROTECTION AND PRIVACY OF HEALTH DATA IN THE CLOUD

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

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

Recommended Citation

Seddon, Jonathan and Currie, Wendy, "INSTITUTIONAL EFFECTS OF COMPARATIVE GOVERNMENT REGULATION FOR THE PROTECTION AND PRIVACY OF HEALTH DATA IN THE CLOUD" in Mola, L., Carugati, A,. Kokkinaki, A., Pouloudi, N., (eds) (2014) *Proceedings of the 8th Mediterranean Conference on Information Systems*, Verona, Italy, September 03-05. CD-ROM. ISBN: 978-88-6787-273-2.
http://aisel.aisnet.org/mcis2014/6

INSTITUTIONAL EFFECTS OF COMPARATIVE GOVERNMENT REGULATION FOR THE PROTECTION AND PRIVACY OF HEALTH DATA IN THE CLOUD

Seddon, Jonathan, Audencia, Nantes School of Management, jonathanseddon1@gmail.com

Currie, Wendy, Audencia, Nantes School of Management, wcurrie@audencia.com

Abstract

This research is a comparative study of the institutional effects of regulatory and compliance issues surrounding cloud computing in healthcare. Our focus is on health care organizations and the IT industry, and how these two important stakeholders interpret and apply the privacy and security rules from the U.S. and EU. As an institutional environment, healthcare is experiencing coercive, normative and mimetic isomorphic pressures on macro, meso and micro levels. International governments are seeking ways to build capacity in the cloud computing market, yet they are faced with difficult issues in relation to privacy and security of personal data. Our findings suggest that regulatory and compliance is being developed 'in response to' rather than 'in anticipation of' technical change. Normative pressures to encourage healthcare organizations to develop effective data protection and privacy policies to comply with new regulatory change are further complicated in an environment where cloud data may be transferred across different legal and regulatory jurisdictions. Our findings show that healthcare organizations and cloud providers need to work more closely together as business associates. However, translating HIPAA and EU rules and regulations into practice is thwarted by a lack of legal and regulatory knowledge, particularly in the smaller organizations.

Keywords: Institutional effects, health data, privacy and security, regulation

1. Introduction

The emerging market of cloud computing poses fresh challenges for policy-makers, healthcare organizations and the IT industry, as health data and information is increasingly transferred across national or state borders where little consensus exists about which authorities have jurisdiction over cloud data (Wolf and Tobin, 2007). This study examines institutional effects of regulation and compliance governing the US and Europe on privacy and security of health data. Based on primary interview and secondary source data, the research reveals the complex challenges facing policy-makers, health care organizations and cloud providers in adopting cloud computing in healthcare environments. As trans-Atlantic regulatory frameworks are developed to keep pace with the fast-moving market in cloud computing, evidence from our data shows that health care organizations and cloud providers need to work together to meet stringent compliance rules to avoid penalties and reputational damage. Traditional sourcing relationships where the cloud provider merely acts as a 'conduit' for personal data are now being replaced with more stringent demands to work with clients as partners or 'business associates' with shared responsibility and accountability for the privacy and security of sensitive health data (DHHS, 2012). Current institutional arrangements in the U.S and Europe which support isomorphic conditions to harmonize regulation and compliance across regions, countries and supra-national states are resisted by contrasting institutional logics about privacy and security of personal (health) data.

The US government and European Union continue the drive towards cloud computing through the use of electronic health records (EHRs).Institutional analysis on the development, maintenance and stability of healthcare systems needs to be extended as new coercive, mimetic and normative (Dimaggio and Powell, 1983, Mizruchi and Fein, 1999) pressures point to further restructuring and even de-institutionalization of current healthcare practices. In this paper, we explore the emerging market of cloud computing within the institutional field of healthcare, focusing on policy-makers, health and IT professionals. As cloud computing enables the transfer of health data across national, regional or state borders, new pressures are placed upon governments, where little consensus exists about which authorities have jurisdiction over cloud data (Berry and Reisman, 2012).At the top of the agenda for challenges in cloud computing is privacy and security. One survey compared findings from the regions of Asia Pacific, Europe and North America on the impediments to adoption of cloud computing. It found that Europe was mostly concerned about privacy and security with over 80% of respondents rating these issues as 'very serious' (World Economic Forum and Accenture, 2009).

Institutional arrangements for governing health data privacy and security differ between the U.S. and Europe. In the US, The Office for Civil Rights enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, protects the privacy of individually identifiable health information. The HIPAA Security Rule sets national standards for the security of electronic protected health information and the confidentiality provisions of the Patient Safety Rule, which protects identifiable information being used to analyse patient safety events and improve patient safety. In comparison, the EU has the Data Protection Directive which regulates the processing of personal data across 28 Member States. It is an important component of EU privacy and human rights law. The Directive was adopted to harmonize national provisions on the protection of individuals in the processing and free movement of personal data. In 2010, the European Commission adopted a Communication setting out a comprehensive approach on personnel data protection in the EU on how to address new challenges to the protection of personal data at EU level and continue to ensure a high level of data protection and the free flow of personal data. In 2012, a draft European General Data Protection Regulation was unveiled to supersede the Data Protection Directive. Data protection is enshrined in the Treaty on the functioning of the EU which observes that all citizens have the right to the protection of their personal data. A comprehensive revision of the current Data Protection Directive aimed 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 a high level of health protection (European Commission, 2012a). Faced with emerging regulation and compliance Directives, laws, policies and practices from the US and Europe, we examine how coercive institutional pressures to prevent health data infringements are acted upon by cloud providers seeking to adopt normative practices to protect personal privacy and security. We further explore mimetic pressures on healthcare organizations to introduce robust governance and compliance practices for controlling and processing cloud-based health data which mirrors other industries, such as financial services. As regulators attempt to keep pace with the fast-moving market in cloud computing, evidence from our data shows that health care organizations and IT providers are increasingly expected to work together to meet stringent compliance rules to avoid penalties and reputational damage. Our institutional approach, however, suggests a more nuanced understanding is needed as coercive regulatory laws and rules are likely to have unintended consequences as their interpretation and monitoring prove difficult as healthcare organizations and cloud providers navigate their way through an increasingly complex global regulatory and compliance environment.

This paper is divided into four parts. First, we give a brief overview of some of the key differences in U.S. and EU policy on cloud computing. We note that while both regions support the development of cloud computing as a vehicle for promoting free trade, enhanced job opportunities and improvements in information and data management in healthcare, two distinct regulatory and policy approaches exist. Second, we discuss our conceptual approach using institutional theory as a lens to examine regulatory and compliance cloud computing challenges for the field of healthcare. Our focus is on two stakeholder groups: health care organizations and IT providers. Under existing and emerging trans-Atlantic regulation, these groups will need to work more closely together to comply with increasingly stringent rules governing the cross-border transfer of health data. Third, we present our findings in the discussion section. We compare U.S. and EU regulatory and compliance frameworks governing privacy and security of health data in the cloud. We offer insights into the key challenges for health care organizations and cloud providers, and recommend areas for further research for the IS community.

2. US and EU Cloud Computing Policy

The global cloud policy and technology landscape is a complex assortment of different legal, regulatory and compliance frameworks and models. Despite calls for a '*global marketplace for cloud computing*' different countries continue to develop and refine their policies on privacy and security, intellectual property, technology interoperability, legal harmonisation, free trade and ICT infrastructure. Global revenues for cloud computing are forecast to grow from a $40.7 billion in 2011 to $241 billion in 2020 (Ried at al, 2011). The market comprises software-as-a-service (SaaS), platform-as-a-service (PaaS), infrastructure-as-a-service (IaaS) and business processes-as-a-service (BpaaS). SaaS is by far the largest market growing from $21.2 billion in 2011 to an estimated $92.8 billion in 2016. Cloud computing is the use of computing resources (hardware and software) that are delivered as a service (e.g. email) over a network (e.g. the Internet). The use of cloud computing in healthcare is particularly contentious since it entrusts remote services provided by IT firms with health data and information.

Four types of cloud computing have emerged in recent years, with differing privacy and security considerations for health care organizations. The Public cloud infrastructure is provisioned for open use by the general public with major players including Amazon and Google. It may be owned, managed, and operated by a business, academic, or government organization, or a combination of these entities. It exists on the premises of the cloud provider. The Community 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. The Hybrid cloud infrastructure comprises 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). The

Private cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). 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. This form of cloud computing is perceived as offering the most safeguards for health care organizations.

In the U.S, the National Institute of Standards and Technology (NIST) supports the government in adopting cloud computing models to reduce costs and improve services. The Federal Cloud Computing Strategy describes this role as, '*..a central one in defining and advancing standards, and collaborating with USG Agency CIOs, private sector experts, and international bodies to identify and reach consensus on cloud computing technology and standardization priorities.*' The NIST Cloud Computing program and initiative aims to develop a Cloud Computing Technology Roadmap complementary to U.S. government initiatives defined in the broader strategy. *"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"* (Mell and Grance, 2011).

In the EU, the Commission presented a European cloud strategy in the form of a communication entitled, 'Unleashing the Potential of Cloud Computing in Europe' (European Commission, 2012a), in which it announced the intention to set up a European Cloud Partnership (ECP). Under the guidance of the Steering Board, the ECP brings together public authorities and industry consortia to advance the objectives of the strategy towards a digital single market for cloud computing. Cloud computing is described as an 'engine for growth'. However, there are calls for a common European regulatory framework, as the current fragmentation inhibits the development of a digital single market for cloud computing. This concerns data location, digital content and data protection laws that span many jurisdictions. The following priorities under two axes are recommended:- 1] Harmonisation measures: the Commission will draft a matrix of challenges to the adoption of cloud computing; 2] Acceleration measures: to reinforce a vision for this work with key performance targets against which it can measure its success. In addition, 'concrete lighthouse proposals' are suggested that show how cloud computing can help to solve major problems in areas of social affairs, growth and jobs, small and medium enterprises (SMEs). One study estimates that cloud computing has the potential to create 1.5 million jobs in Europe by 2015, with a turnover worldwide in 2010 of around €26 billion. Neelie Kroes, commissioner for the digital agenda, estimates the savings from cloud computing could be around €300 per person per year. Other estimates claim that expected gains could be around €600 billion between 2015 and 2020. Smaller businesses are expected to benefit with forecasted savings of some 10-20% in ICT, due to lower total costs of ownership (TCO) of using cloud computing (European Commission, 2012b). Like the US, the European Commission is making Cloud computing an important political priority.

3. Conceptual Underpinnings

As a concept and a practice, cloud computing in healthcare necessitates a wider macro, meso and micro level analysis, as environmental, organizational and individual inputs are all part of the mix. At the institutional environmental level, national and supranational governments are concerned to develop regulatory and compliance policies to encourage structural isomorphism, e.g. the need for all actors in the healthcare field to conform to a single archetype or structural model (Boxenbaum and Jonsson, 2008). All actors performing a similar function may reflect the same basic structural features in their organizational design. Conversely, organizational actors may embrace many diverse structural templates (Scott et al, 2000, 359). Currently, the international cloud computing market suggests the latter, where adoption and diffusion practices differ across nation states. For example, Japan, Australia, the US and Europe, all have different legal and regulatory systems, with diffusion levels of cloud computing steadily increasing (Martin, 2012). However, different institutional arrangements and logics exist in regard to privacy and security of cloud data. Comparing the U.S. and Europe, two distinct approaches to privacy and security are seen, with variations in regulative, normative and cultural cognitive structures, values, social norms, and interests (Scott, 2001).

Institutional environments, arrangements and logics are becoming more complex in the U.S. and EU as outsourcing arrangements for cloud-based models increasingly conflate client and vendor responsibility and accountability (Marston et al, 2011,). Health data in the cloud may be transferred across national, regional/state borders. While the US has a national policy framework in the form of HIPAA, the EU comprises 28 Member States, each with their own national government and even regional policies covering health data. Within the EU, little consensus exists over which national authorities have jurisdiction over cloud data, with countries like Germany having very stringent health data laws and policies and other EU member states having less stringent rules. This is further complicated when health data is transferred outside the EU by an IT provider with data centres in various geographical locations. Industry standards pertaining to administrative, physical and technical safeguards for health data also vary across countries and organizations. These safeguards are enshrined in HIPAA regulation and the EU Data protection Directive with varying points of emphasis.

As institutional actors make sense of new regulatory requirements, roles and responsibilities between healthcare organizations and IT providers are becoming more intertwined. An illustration is in cloud computing contracts where healthcare organizations are encouraged to treat IT providers as 'Business Associates' (BAs). HIPAA defines a business associate is *"any organization or person working in association with or providing services to a covered entity who handles or discloses Personal Health Information (PHI) or Personal Health Records (PHI)*" (DHHS, 2012). Examples are accounting or consulting firms who work in health care organizations, including clinical and non-clinical staff with access to PHIs or PHRs. Similarly in Europe, the demarcation is made between a data controller and a data processor. The data controller determines *'who is responsible for compliance and data protection rules, and how data subjects can exercise the rights in practice*', e.g. to allocate responsibility. The data processor is, 'the natural or legal person, public authority or agency or any other body that alone or jointly with others, processes personal data on behalf of the controller' (European Commission, 2012, 7-8). Adopting an institutionalist perspective, this paper is interested to observe how institutional environments, arrangements and logics effect the regulation of health data using cloud computing across the U.S and EU. Institutional concepts of coercive, mimetic and normative pressures offer a lens to examine how governments, healthcare organizations and IT providers make sense of regulatory regimes across field boundaries with different institutional structures and practices. We next discuss our data collection methods.

3.1. Data collection methods

The research study is a comparative analysis of U.S and EU regulation and compliance policy for cloud computing in healthcare. While there are many cross-field studies within institutional theory, there is a lack of cross-national studies, where different logics emanating from multiple macro, meso and micro levels may collide culminating in unintended consequences and outcomes. Our study addresses this gap within the institutional theory literature by providing insights on how Directives, laws and rules surrounding the emerging market of cloud computing are interpreted and applied in different countries and across regions/states. Our notion of field therefore extends beyond national borders by considering how emerging technology used within the healthcare domain is governed not simply by organizational strategies but by cross-jurisdictional laws and directives. So far, the technical development of cloud computing far out-strips the progress of the regulatory and compliance regime. However, concerns about privacy and security among health care organizations act as barriers for many healthcare organizations in moving heath data onto the cloud [Chow et al, 2009]. Primary and secondary data was collected over a two year period. Semi-structured interviews were carried out with 28 health professionals (12 interviews with U.S. informants and 16 interviews with European informants) to gather data on regulatory and compliance challenges of cloud computing in health care organizations. In addition, 15 interviews were carried out with IT vendors who offer cloud computing products and services to the health sector. The interviews lasted around 55 minutes. The broad research questions were: *What is the regulatory framework for cloud computing in the US and Europe? and, How will healthcare organizations and the IT industry develop compliance policies and practices to meet these changes?*

In addition to primary interviews, secondary source data was collected and analysed from a range of government, IT industry, NGO and health care organizations (hospitals, patient groups and associations, among others). This information provides a valuable source of material on both the generic issues surround cloud computing and the specific issues facing health care organizations and the IT industry.

4. Discussion and Analysis

A comparative analysis of the U.S and EU regulation and compliance policies and practices in the context of cloud computing in healthcare reveals wide differences. Distinct approaches to privacy and security are seen, with variations in values, social norms, and interests accounting for much of these differences. In the U.S, the concept or privacy is not written into the Constitution, so the right to privacy of the citizen is not wholly guaranteed. The history of privacy regulations in the U.S has focused around industry self-regulation and reactive legislation. The U.S approach is described as laissez-faire with markets setting the agenda, and governments intervening only when the private sector falls short. By contrast, the EU has proactively regulated the use of personal data, where the state is seen as playing an important role in protecting the rights of citizens' privacy and security. By extension, the EU requires close participation between business and government in discussing regulatory and compliance issues with the interests of the citizen at the centre. The right to privacy is seen more as a human right, with the governments of many EU countries embedding privacy in their Constitutions (e.g. Germany and Spain), and more widely in the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms. The Treaty to establish a Constitution for Europe further states the importance of strengthening the protection of fundamental rights following social and technological changes (Movius and Krup, 2009).

Our data highlights different approaches towards regulation and compliance by the U.S and EU. Institutional arrangements and logics on how health organizations and IT providers interpret and implement laws and rules suggest a lack of harmonization, particularly in the area of health data privacy and security. We discuss the two distinct approaches in more detail.

4.1 US Regulation and Compliance

The U.S. government promotes health IT as part of the HITECH Act (Health Information Technology for Economic and Clinical Health) of 2009. The government pledged a $787 billion stimulus package to develop electronic health records (EHRs) for healthcare. One element of the Act was to ensure that healthcare organizations would work more closely with IT providers, not simply as part of a client-provider split, but as partners. So under the U.S. Health Insurance Portability and Accountability Act of 1996, a HIPAA business associate agreement (BAA) is a type of outsourcing contract between a HIPAA covered entity and a HIPAA business associate (BA). The contract protects personal health information (PHI) in accordance with the guidelines. Since 2010, outlined in the HITECH Act, a BA's disclosure, handling and use of PHI must comply with HIPAA Security Rule and HIPAA Privacy Rule mandates. A BA that serves a health care provider or institution is now subject to audits by the Office for Civil Rights (OCR) within the Department of Health and Human Services and can be held accountable for a data breach and penalized for non-compliance. These new regulations force the BA to explicitly state how they will report and respond to a data breach, including data breaches resulting from a BA's subcontractors. Also, BA's are required to show how they will respond to an OCR investigation.

A recent case saw the United States Department of Health & Human Services (DHHS) Office for Civil Rights (OCR) agreeing a $100,000 monetary settlement with Phoenix Cardiac Surgery, P.C. (PCS) alleging various violations of the HIPAA privacy and security rules. Violations included a failure to: implement adequate policies and procedures to appropriately safeguard patient information; document that it trained any employees on its policies and procedures on the Privacy and Security Rules; identify a security official and conduct a risk analysis; and obtain business associate agreements with Internet-based email and calendar services where the provision of the service included storage of and access to its ePHI. The PCS settlement followed an extensive three-year investigation, stemming from allegations that PCS posted patients' clinical and surgical appointments on a publicly accessible Internet-based calendar. It was also alleged that PCS transmitted electronic PHI from an Internet-based email account to employees' personal Internet-based email accounts. In addition to the financial settlement, PCS will implement a corrective action plan that includes a review of recently developed policies and other actions taken to come into full compliance with the Privacy and Security Rules. The OCR which has HIPAA enforcement authority offered a public statement about the Phoenix Cardiac Surgery case: "If you use a cloud service, it should be your business associate. If they refuse to sign a business associate agreement, don't use the cloud service." Reporting of violations of the HIPAA Privacy Rule is invited by the US Department of Health and Human Services (DHHS)….." If you believe that a covered entity violated your (or someone else's) health information privacy rights or committed another violation of the HIPAA Privacy Rule, you may file a HIPAA Privacy Rule Complaint with OCR".

The HIPAA Privacy Rule extends beyond the large health care organization to encapsulate small GP/physician practices with access to PHI. Patients are encouraged to be vigilant about protecting their health data, so mechanisms to report violations if they feel their privacy is being breached are in place. Physicians are not exempt from responsibility so they need to understand how if using their personal email (e.g. Gmail, Yahoo, Hotmail or AOL account for office business) complies with the privacy and security rules. Since physicians often work in a mobile capacity using their hand-held devices (e.g. mobile phones), it is the potential for violations are increased (e.g. using personal email to sign off patients, discuss appointments, test results, etc). Within the HIPAA rules, non-secured email services for transferring patient health data amount to violations.

From our interview data with US physicians, concerns were raised about the lack of awareness about HIPAA. One physician claimed, "*The HIPAA rules have been brought in over the past few years and we, as a profession, have to comply or face heavy penalties. We need to work with our IT vendors as partners and not just buy a cloud service and think we can carry on as business-as-usual*".

Interviews with cloud service providers suggested that some were confused about their role as BAs, since they perceived their role more as a conduit for health data to be stored or transferred through their data center. However, the updated HIPAA Privacy and Security rules released in 2013, reject this view if the cloud vendor maintains protected health information in their cloud data center. Thus, "an entity that maintains protected health information on behalf of a covered entity is a business associate and not a conduit, even if the entity does not actually view the protected health information...a data storage company that has access to protected health information (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis. …To help clarify this point, we have modified the definition of "business associate" to generally provide that a business associate includes a person who "creates, receives, maintains, or transmits" (emphasis added) protected health information on behalf of a covered entity. (Federal Register 25-26).

For cloud providers, the HIPAA regulations impose stringent penalties and fines for non-compliance which cascade down to other firms acting as sub-contractors. A central issue for cloud providers, not just in the U.S, but internationally, is that platforms, infrastructure, business processes, and applications will all need to comply with privacy and security rules concerning the storage and transfer of health data. For example, cloud services for EHRs will be constrained by federal regulatory legislation and oversight (Schweitzer, 2013, p.161).While the U.S. has traditionally seen privacy rights falling within self-regulation and governance, the potential for cloud computing in healthcare to span many jurisdictions will necessitate the need to harmonize or at least co-operate with differing legal and regulatory systems.

4.2 EU Regulation and Compliance

The EU Data Privacy Directive develops standards which the 27 Member States must embed into their own national data privacy and security laws. These standards apply when either a company or individual collects health data on an EU citizen. The EU directive has far-reaching international implications. For example, US health organizations must comply with the Directive if they collect health data on EU citizens (Berry and Reisman, 2012). Since cloud computing is likely to involve the cross-border transfer of health data, the Commission has concerns that some U.S. IT vendors who control this data may not meet the regulative and legal requirements set out in the Directive. The EU prohibits the export of personal (health) data unless the importing country 'ensures an adequate level of protection' (Wolf and Tobin, 2007). The U.S. is not currently among the nine countries that have been recognized. However, the EU and U.S. have developed a compromise, called the 'Safe Harbor' provision. This enables the U.S. to voluntarily self-certify that they meet the requirements of the Directive. This allows U.S. firms to qualify individually even though the country, as a whole, does not qualify.

Within the EU more generally, the Data Privacy Directive intends that a uniform standard of data protection is in place throughout the EU. In practice, however, variation exists in how the 28 Member States interpret and implement the Directive. In Germany, for example, many healthcare organizations do not permit health data to be stored outside the physical premises, making cloud computing a non-viable option. In other EU countries, notably, the U.K. the development of a national program for EHRs has been met with serious resistance, from clinicians and their representative bodies, particularly as fears about access rights and transfer of electronic patient data is viewed as a potential threat to patient security and confidentiality (Currie, 2012).

Proposals to alter the EU data protection rules have been questioned by leading medical bodies, such as the British Medical Association (BMA). Doctors fear that changes could put existing patient confidentiality safeguards at risk. Draft proposals on the processing and free movement of personal information suggest that identifiable health data could be used for research without patient consent. The BMA is concerned that the provisions will remove current patient confidentiality safeguards and allow identifiable health data to be used without consent for historical, statistical or scientific research purposes when anonymized or pseudonymized data cannot be used. Although the regulation states that data that could reveal identities must be segregated, greater clarification is needed about whether this could be on separate databases, or transferred outside the organizations where it was initially stored. An interview with one UK-based senior doctor stressed, "*The problem with the current regulatory regime concerning health data privacy and security is that legislation and policy is not in line with medical and technical progress. Politicians and legislators are trying to keep up with advances in medicine, such as genome mapping and developments in IT, such as cloud computing. Unfortunately, we are now seeing a patch-work quilt of different and incompatible rules and regulations, with mixed messages about incentives and penalties for compliance and non-compliance'.*

BMA's Director General said, 'The BMA has serious concerns that Article 83 appears to permit the processing of health data, in identifiable form, for research purposes without any reference to consent…The only safeguards which appear in the clause seem to be that identifiable data must be kept separate, and researchers can use (it) only if research cannot be fulfilled by using non-identifiable data. This seems to be significantly lower than the existing standard for protection of health data' (BMA, 2012). The BMA, however, recognizes the EU Directive needs to be updated given the technological advances and changes to consent provisions. The proposal to shorten the time data controllers have to respond to subject access requests from 40 days to 30 days will be an administrative burden. Clarity is therefore needed over whether GP practices and clinical commissioning groups could be fined if records are not provided in a portable electronic format to patients. Coercive pressures to improve the process of subject access requests will have significant implications for health care organizations and cloud providers, not least because the punitive action may be taken if regulators discover infringements in relation to how patient records are stored and transferred.

4.3 Institutional effects of regulating health data in the cloud

The institutional effects of regulating health data in the cloud are inherently complex as trans-border data flows encounter different institutional environments, arrangements and logics. U.S. and EU policy-makers and legislators support the move towards cloud computing as a potential means of improving health service delivery, yet the coercive, mimetic and normative pressures governing health data vary widely. While the U.S. is less concerned with privacy as a human right, compared with the EU, the HIPAA Privacy and Security Rules impose serious penalties and fines for violations and breaches, such as the case of Phoenix Cardiac Surgery discussed above. These coercive pressures are likely to produce mixed outcomes. Healthcare organizations engaging in normative behaviors to improve their professional practices are likely to increase legitimization of how health data is governed. This may encourage other healthcare organizations to mimic these organizations, suggesting isomorphic change in line with the requirements of the regulator. However, these coercive, normative and mimetic isomorphic pressures may slow the pace of cloud computing in healthcare, where penalties and sanctions result in reputational damage for healthcare organizations and IT providers.

An example is found in the EU where the Commission recently launched an investigation against Google over allegations that it is abusing users' personal data (Doyle, 2013). Within the EU there are six data protection regulators. An investigation was launched by 29 European agencies to examine Google's decision to pool anonymous data across Google services, which may benefit the company in selling online advertisements. Google and other large internet firms like Facebook provide free services to consumers and earn revenues from selling ads which they claim are targeted to individual interests unlike the more traditional approaches used in television and radio. While this investigation is about the broader issue of users' personal data, the implications for cloud providers working with healthcare organizations are significant. Yet coercive pressures by the EU to force multi-national companies to adhere to stringent regulations are made more challenging due to the lack of international harmonization of regulatory and legal systems. Regulators are therefore 'behind the curve' of the business and IT strategies of large firms so exercising laws and rules is more likely to be effective with the smaller players.

Within the institutional environment, the various trans-Atlantic regulatory and compliance approaches, such as, the EU Data Privacy Directive, EU Model Clauses, EU Safe Harbor, ISO 27001 (International Organization for Standardization), the U.S. FISMA (Federal Information Security Management Act), HIPAA, Business Associate Agreements (BAAs) Data Processing Agreements, and binding corporate rules (BCRs) all attract support and criticism from the communities they serve. Conflicting institutional arrangements and logics exist within the international healthcare field. One area which is being tackled by the regulator is about access the health data. One question surrounding cloud computing is: *who has access to health data?* In the EU, the notion of model contract clauses and binding corporate rules (BCRs) as institutional mechanisms for processing personal data in the cloud is contentious, not least because these arrangements do not prohibit U.S. law enforcement bodies from gaining access to this data. A report, ordered by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) (European Commission, 2012c), claimed that the EU had created "derogations" from traditional rules governing international transfers of personal data, which, in the context of cloud computing, could not adequately protect the privacy of the data. The BCRs and model contract clauses were examples of the 'derogations' created and that both are were ‘equally unsuitable to prevent the use of cloud data for surveillance purposes’. It said the EU had made ‘errors’ when forging an agreement with the US over the recognition of U.S. organisations' data protection standards.

The terms of the EU's 'Safe Harbor' agreement with the U.S. mean that the EU cannot control who can access EU citizens' personal data once it has been uploaded to cloud servers. The existing derogations must be dis-applied for Cloud due to the systemic risk of loss of data sovereignty. It stressed the EU should enter into fresh negotiations with the U.S. for the recognition of a human right to privacy where Europeans are granted equal protections in U.S. courts. The US-EU Safe Harbor agreement allows for such data transfers where data protections meet EU standards. U.S. organizations that conform to requirements of the scheme are believed to have satisfied European safety standards outlined in the Data Protection Directive. Under this Directive companies are prohibited from sending personal data outside of the European Economic Area (EEA) unless robust protections have been put in place, or where the destination country has been designated as possessing adequate data protection.

For countries outside the EEA, labelled as ‘third’ countries, a company needs to show that robust protections are in place, which means the data is given the same protection under EU laws. The report claims that U.S. authorities could ‘lawfully’ obtain access to EU citizens' personal data on cloud servers under the terms of the U.S. Patriot Act or U.S. Foreign Intelligence Surveillance Amendment (FISA) Act. This means the EU's exclusive sovereignty over the data is lost once it transfers onto cloud servers. Such a move reduces the impact of BCRs and model contract clauses. The report stresses that planned revisions to the EU's data protection law framework should include rules governing ‘law enforcement cooperation with the private sector’. It recommends the European Parliament develops a revised framework where companies give ‘prominent warnings to individual data subjects’ to inform them that EU cloud data could be ‘exported to US jurisdiction’.

Our findings suggest the institutional field of healthcare is a complex array of existing and emerging privacy and security regulations. At the level of the health care organization, negotiations with cloud providers need to address the how health data will be governed if it is transferred across legal and regulatory different jurisdictions. Our interviews with cloud providers uncovered a range of issues about the importance of complying with current U.S. and EU privacy and security rules, but also concerns about possible violations and sanctions. One cloud provider commented, *“My company offers cloud services for EHRs. We are now moving to the cloud but apart from using an outsourced legal team, we are not fully aware of all the rules and regulations. The lawyers are going to make a lot of money out of the cloud computing industry…..but the penalties for data violations will be met by the client and possibly the IT vendor. More education is needed about this space as regulations are being developed in an adhoc way”* (SME IT provider, London, UK).

While U.S. HIPAA regulation seeks to expose those who do not fully comply with privacy and security rules, the E.U. under the Article 29 Working Party, formed an opinion that EU organizations using cloud computing to store and process personal data must use cloud providers that can ‘guarantee’ compliance with EU data protection laws. It cautions against cloud providers' "self-certification" suggesting they comply with U.S-EU Safe Harbor standards, which may not fully comply with EU data protection laws. For example, cloud providers that operate as either a 'platform-as-a-service' (PaaS) or 'software-as-a-service' (SaaS) may not meet the privacy principles on which Safe Harbour is founded since they are largely ‘conduits’ of data or data processors. Data processors that obtain BCRs are challenged by similar constraints over the privacy protections they claim when processing health data in the cloud. Yet the use of auditing schemes to review cloud providers' data protection standards does not resolve those constraints. Safe Harbour for processors is a problematic concept (because a IaaS/PaaS Cloud cannot by definition fulfil any of the Safe Harbour Agreement Principles). Further, BCRs for processors may not guarantee that sensitive data will not be accessed by governments in other jurisdictions.

Despite the attempts by the E.U to recommend robust audit procedures to ensure cloud services are compliant, there currently exists no reliable commercial audit methodology that can fully protect personal or health data. Once data is transferred to the cloud, it is difficult for healthcare organizations to uncover covert surveillance whether this is 'lawful' under the national security rubric of a third country (especially if that audit is conducted by a company from that country). So the notion of a Data Processing Agreement being able to cover this scenario is not possible, particularly if the Cloud provider operates outside the EU jurisdiction. The European Commission has now developed new model contract terms for organizations who wish to enter into contracts and service level agreements with cloud providers.

Other areas which fall within the regulatory and compliance arena are on-demand (24/7) access to health data. The so-called ‘anytime, any place, anywhere’ promise of data access is an important market logic for cloud computing, particularly where easy access to patient data may be required in an emergency scenario. Normative pressures for IT vendors to embed into their cloud offerings a range of regulative and compliance measures, including, the Data Processing Agreement, EU Model Clauses, EU Safe Harbor, HIPAA, with Business Associate Agreement (BAA), FISMA (Federal Information Security Management Act), and ISO 27001 (International Organization for Standardization) are all examples of coercive pressures. However, institutional arrangements across national states differ in relation to standards. Healthcare organizations may unwittingly enter into agreements with cloud providers who are unable to demonstrate they have stringent policies which adhere to industry standards. Normative pressures about which standards to adopt are likely to confuse smaller cloud providers, particularly where they lack the legal awareness to evaluate their rights and responsibilities in controlling and processing health data in the cloud.

Ethical uses of health data are a further factor which is becoming increasingly important. How health data is governed extends beyond the technical remit to include potential commercial exploitation and use of personal data. The likelihood of ‘data mingling’ (where health data is sent through a public cloud, where data co-mingles with other companies’ data) may occur. This is reduced in the private cloud where there is no shared infrastructure and less risk of data co-mingling with other entities.

5. Conclusion

This research is a comparative study of the institutional effects of regulatory and compliance issues surrounding cloud computing in healthcare. Our focus is on health care organizations and the IT industry, and how these two important stakeholders interpret and apply the privacy and security rules from the U.S. and EU. As an institutional environment, healthcare is experiencing coercive, normative and mimetic isomorphic pressures on macro, meso and micro levels. International governments are seeking ways to build capacity in the cloud computing market, yet they are faced with difficult issues in relation to privacy and security of personal data (Venters and Whitley, 2012). Our findings suggest that regulatory and compliance is being developed ‘in response to’ rather than ‘in anticipation of’ technical change. Normative pressures to encourage healthcare organizations to develop effective data protection and privacy policies to comply with new regulatory change are complicated in an environment where cloud data may be transferred across different legal and regulatory jurisdictions. Healthcare organizations and cloud providers are encouraged to work together as business associates, although translating HIPAA and EU rules and regulations into practice is thwarted by a lack of legal and regulatory knowledge, particularly in the smaller organizations. At the micro level, the notion that citizens should be made fully aware if their sensitive health data is exposed to the ‘surveillance apparatus’ of another country is shared by many, yet guaranteed by few, as key stakeholders (e.g. policy-makers, health professionals, IT firms) negotiate cloud policy and implementation.

The issues surrounding cloud computing in healthcare are complex and challenging, particularly as health care organizations, who may have low competencies in IT (compared with other sectors like finance) now seek to enter into contracts with cloud providers. Our findings support a more nuanced approach embracing comparative research on regulatory measures from HIPAA in the U.S. to the Data Protection Directive in the EU. These regulations developed at the country and pan-European levels respectively present policy-makers with serious challenges where sensitive health data is transferred across organizational, state (regional) and country boundaries. While leading IT firms, such as Microsoft, have developed their Windows 365 to be HIPAA compliant, healthcare organizations face potential threats if they use cloud services from non-HIPAA compliant vendors. Stringent privacy and security rules underpinning this legislation pose further challenges as any healthcare organization using an external IT provider must now ascertain whether all sub-contracted parties also comply. Since this is a relatively new development in outsourced IT contracts (e.g. using cloud services for email and document management) the regulation now assumes that cloud providers can no longer be mere ‘conduits’ of health data, but are in fact, business associates, subject to the same compliance rules as their clients. Findings from this research, however, suggest that competencies and know-how about the intersection between regulation and compliance for cloud computing in healthcare remain low. Hospital IT staff are generally trained in negotiating outsourcing contracts with local or national suppliers, yet their knowledge of national, pan-European or even trans-Atlantic legal and regulatory frameworks for cloud computing is limited. Signing a standard IT outsourcing contract is therefore risky, particularly as the cloud provider may also demonstrate limited awareness of the requirements outlined in either HIPAA or EU data privacy laws.

In summary, the institutional effects of comparative government regulation for the protection and privacy of health data in the cloud extends beyond the business, organizational and technical domain (Marston et al, 2001; Sultan, 2013). Since cloud computing spans multiple disciplines and industry sectors, research into this field needs to consider, not just the IT artefact, but also, how clients of cloud services enter into agreements with cloud providers where stringent regulatory and compliance obligations govern not just the success or failure of delivery a cloud-based business process or service, but whether such a contract will ultimately violate U.S. or EU privacy and security laws. Despite data protection policies starting out as general statements, their interpretation and application also depends on the institutional social norms, culture and values of a country or even professional group. Understanding how different countries adopt cloud solutions is an interesting research challenge for the IS community. Equally, how different professional groups move to the cloud is also illuminating. Within healthcare, the promise of technology to improve health service delivery is met with fresh opportunities, given the burgeoning health IT sector, but also serious barriers, as health professionals grapple with the complex arena of new medical devices, applications and infrastructure. This study offers a high level analysis and suggests the need for more cross-national IS research which considers how emerging technologies, such as cloud computing is adopted by healthcare organizations in a global regulatory environment. It also offers a cautionary note to practitioners, who are keen to develop and sell their health IT solutions, albeit now in an environment where privacy and security issues surrounding health data possibly outweigh other considerations such as cost reduction.

References

Alshamaila, Y., Papagiannidis, S. (2012) ‘Cloud computing adoption by SMEs in the north east of England’. Journal of Enterprise Information Management. 26:3, pp. 250-275.

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

Boxenbaum, E. and Jonsson, S. (2008) ‘Isomorphism, Diffusion and Decoupling’, in R. Greenwood, C. Oliver, K. Sahlin and R. Suddaby (eds) The SAGE Handbook of Organizational Institutionalism, 78-98. Los Angeles, SAGE.

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, USA.ACM 978-1-60558-784-4/09/11.

Currie, W. (2012) Institutional isomorphism and change: the national programme for IT – 10 years on. Journal of Information Technology, 27, 236-248.

Department of Health & Human Services (2012) www.hhs.gov/ocr.

Dimaggio, P.J. and Powell, W.W. (1983) "The iron cage revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields". American Sociological Review, 48:2, 147-160.

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

European Commission (2012b) 'Digital Agenda: Tech CEOs and leaderskickstart new EU cloud computing board'. IP/12/1225. (http://www.euractiv.com/infosociety/brussels-unveils-cloud-computing-news-515057).

European Commission (2012c) Fighting cyber crime and protecting privacy in the cloud.Citizens Rights and Constitutional Affairs.www. Europarl.europa.eu/studies.

Ried, S., Kisker, H.,withMatzke,P.,Bartels, A., Lisserman, M (2011) Sizing the Cloud: A BT Futures Report. Forrester Research.

Hiller, J., McMullen, M.S., Chummey, W.M. and Baumer, D.L. (2001) Privacy and security in the implementation of Health Information Technology (EHRs): U.S. and EU compared. B.U.J. Sci. & Tech. Journal, 17:1, Winter. Online.

Hupperich, T., Lohr, H., Sadeghi, A.R., Winandy, M. (2012) 'Flexible patient-controlled security for Electronic Health Records'.2nd ACM SIGHIT International Health Informatics Symposium (IHI 2012).

Information Week (2011) Healthcare IT spending to reach $40 Billion.

Lohr, H., Sadhegi, A.R., Winandy, M (2010) 'Securing the E-Health Cloud. IHI'10.November 11-12, Arlington, Virginia, USA.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.

Martin, R (2012) Japan is best prepared to capitalize on cloud computing. http://www.techinasia.com/japan-cloud-cloud-computing/

Mizruchi, M.S. and L. C. Fein, (1999) "The social construction of organizational knowledge: A study of coercive, mimetic and normative isomorphism". Administrative Science Quarterly, 33: 194-210.

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

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).

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).

Scott, R. (2001) Institutions and Organization. Sage, London.

Stahl, B.C., Doherty, N.F., Shaw, M. (2011) 'Information Security Policies in the UK Healthcare Sector: a critical evaluation. Information Systems Journal, 22, 77-94.

Sultan, N. (2013) 'Knowledge management in the age of cloud computing and Web 2.0: Experiencing the power of disruptive innovations'. International Journal of Information Management, 22, 160-165.

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.

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