Published in Availability, Reliability and Security (ARES), 2014 Ninth International Conference on , pp.158-165, 8-12 Sept. 2014, doi: 10.1109/ARES.2014.28
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6980277&isnumber=6980232

Healthcare Services in the Cloud - Obstacles to Adoption, and a Way Forward

Karin Bernsmed, Daniela Soares Cruzes, Martin Gilje Jaatun, Børge Haugset and Erlend Andreas Gjære
Department of Software Engineering, Safety and Security
SINTEF ICT
Trondheim, Norway
{Karin.Bernsmed, daniela.s.cruzes, Martin.G.Jaatun, Borge.Haugset, erlendandreas.gjare}@sintef.no

***Abstract*—Cloud computing has been receiving a great deal of attention during the past few years. A major feature of public cloud services is that data are processed remotely in unknown systems that the users do not own or operate. This context creates a number of challenges related to data privacy and security and may hinder the adoption of cloud technology in, for example, the healthcare domain. This paper presents results from a stakeholder elicitation activity, in which the participants identified a number of obstacles to the adoption of cloud computing for the processing of healthcare data. We compare our results with previous studies and outline accountability as a possible way forward to increase the adoption of cloud services in the healthcare domain**

***Index Terms*—healthcare, cloud, security, privacy, accountability, openspace**

I. Introduction

Cloud computing has been a hot topic in both industry and research for several years, and is now becoming mainstream to the extent that public cloud services can be found everywhere, offering all sorts of IT services in an on-demand and scalable manner. It is thus only natural that cloud computing should be used as a component in all kinds of service delivery, also in the healthcare sector.

In recent years there has been a signicant growth in the use of wireless sensor networks in healthcare [1], [2], which for example can be used for early detection of clinical deterioration through real-time patient monitoring in hospitals or at home, in order to improve the quality of life for the elderly through smart environments, and for monitoring of chronic diseases. The cloud is a preferred solution for analysis and storage of data from medical sensor networks; not only because of cost advantages, but also because of scalability and elasticity requirements. However, while implementing medical sensor networks in the cloud may be preferable from a technical point of view, the off-premises processing of medical data gives rise to a number of issues, in particular in Europe where the right to privacy is a highly developed area. According to the European Data Protection Directive [3], medical data are classified as *sensitive personal data* and are hence subject to strong restrictions regarding collection, usage and further distribution. The processing of healthcare data in the cloud will therefore require particular attention to personal data protection in accordance to relevant legislation, as well as the support of strong privacy by design mechanisms [4]. However, being compliant with legislation is not enough. For cloud computing to be successfully embraced by the decision-makers in the healthcare domain, their point of views and their possible objections to the adoption of new technology first need to be carefully mapped and analysed.

Previous research has explored the potential of cloud computing, and how it can be used to improve healthcare services in, for example, Canada [5], UK [6] and Taiwan [7]. There are several studies that emphasize the way technology plays a role in the adoption of cloud services, and most of these studies conclude that the most important challenges are related to security, privacy and compliance [8], [9], [10], [11], [12].

In this paper we focus on personal data protection issues, and we pay particular attention to the obstacles perceived by patients, hospitals, regulators and service providers with respect to outsourcing the processing of healthcare data to public cloud service providers. To gather new insights, we organised a workshop that consisted of three introductionary presentations, which were then followed by a number of focus group sessions that involved a number of stakeholders from the Norwegian healthcare sector. This paper outlines a number of obstacles to adoption of public cloud services in the healthcare domain identified by the workshop participants, discusses our results in light of the previous studies, and outlines how current research on cloud accountability may help to solve the identified obstacles.

The rest of the paper is organised as follows. Section II explains the methodology that we used to elicit the views of the stakeholders. Section III outlines the use case that was presented to them before the discussions started. In Section IV we present the main obstacles as they were expressed by the stakeholders. Section V provides a discussion of the results, and summarises other relevant work on opportunities and challenges for cloud computing in eHealth. Section VI outlines accountability as a way forward. Finally Section VII concludes the paper.

II. Methodology

A *focus group* is a group discussion on a given topic, which is monitored, facilitated and recorded by a researcher [13], [14]. It is a method that provides a better understanding of how people think about an issue, a practice, a product or a service. In essence, the researcher provides the focus of the discussion,

but the data itself comes from the group interaction. The key steps in a focus group based research process include the following [15]: (A) defining the research questions related to a research problem; (B) planning the focus group session(s) and selecting the participants; (C) executing the session(s), (D) analysing the data, and (E) reporting the results. In this section we present the way in which we implemented these steps in our specific setting.

A. Focus Group Questions

The purpose of our focus group study was to evaluate the challenges that stakeholders in the Norwegian healthcare domain foresee in the scenario of healthcare data in the cloud. More specifically, we were interested in the *obstacles to adoption of public cloud services*, as they were perceived by the participating stakeholders. We wanted to extract challenges from a wide perspective, and we therefore chose to organise the discussions based on the patients', the hospitals', the healthcare service providers' as well as the regulators' and authorities' points of view. There was also a room reserved for open questions, where the participants could choose any other topics or perspectives that they wanted to discuss. To get the participants started and to ease the flow of the discussions we prepared a set of questions in advance (See Table I), which were used as a basis for the discussions at the different sessions.

B. Planning the Sessions

The focus group sessions were run with people that enrolled in an after-hours workshop called "Healthcare data in the Cloud", which focused on security and privacy issues associated with cloud computing in general and health care data in particular. 52 stakeholders from the healthcare sector in Norway attended the workshop and around 40 of these participated in the following focus group sessions. Most of the stakeholders had an industrial background, and some of them were government employees.

The sessions were distributed as shown in Table II. Each participant was allowed to choose where he/she would like to contribute for 20 minutes at a time. Thus, each participant could potentially participate in the discussions from maximum three different perspectives. Each room had a capacity of around 7 to 10 people.

C. Process Execution

Before opening the discussion sessions there were three presentations about healthcare data in the cloud. In one of them the first author of this paper presented the use case that was later used as input to the discussions (c.f. Section III). To focus the discussions, during the focus group sessions all the participants had the list of questions in Table I and the illustration in Fig. 1 printed for reference.

The moderators/facilitators of the sessions were experienced researchers in empirical methods and/or in security research. All the moderators/ facilitators met the day before in order to synchronize the organisation of the sessions, so the sessions would be as uniform as possible. Their responsibilities were to review the feedback from the participants and to facilitate the discussions, to ask questions and to make sure that all participants had a chance to express their opinions. All moderators were also asked to write down a debriefing of the session as soon as possible after their sessions were finished. The debriefing had the following main topics to take notes: 1) the number of participants in the group, 2) whether all participants involved were able to verbalize their thoughts, 3) the main profile of the participants, 4) any conflicting thoughts (when people become animated because they disagree or see things differently), 5) memorable quotes (when someone says something in a way that is moving, insightful, or otherwise striking), 6) interesting/key points (topics that people focused on and what were the main ideas, 7) what was surprising (and not surprising) to the observer, 8) the two or three most valuable things that the observer learned in this focus group, and finally 9) any other observations.

D. Analysing the Results

The day after the execution of the focus group sessions all moderators met to discuss the main results from the discussions focusing on the challenges and opportunities that were mentioned in the discussions and impressions on the participants' views of the topic. Each moderator also wrote a report on his session based on his notes, and these were used for analysing the results.

E. Reporting the Results

In this paper we have extracted and summarised the main obstacles to adoption of a cloud-based solution for healthcare data (such as the one in Fig. 1) that were expressed by the participants in the focus group session. The identified obstacles will be presented in Section IV.

III. Use Case - the M Platform

The healthcare system that was presented to the stakeholders before the start of the focus group sessions is the "M Platform" illustrated in Fig. 1, which is a cloud-based platform for medical sensor data collection, processing, storage and visualization[1]. Patients will be connected to wireless sensors that monitor their vital signs (e.g., movement, blood pressure, pulse oximetry, temperature, position, etc.). The sensor data will be transmitted to the cloud where they will be further processed and stored. The "M Platform" is assumed to be developed by a software and service provider M, which will outsource to one or more external cloud providers both the sensor data collection and initial processing tasks (Cloud x, provided by X) as well as the long-term data storage and back-up procedures (Cloud y, provided by Y). M therefore has a contract with X, and a separate contract with Y. The actual sensors themselves will be deployed by the hospital, which engages M to provide the platform, under a contract between the hospital and M; the hospital has no direct contractual relationship with either

[1]Note that the "M Platform" is currently only a design; no implementation exists.

Perspective	Set of initial discussion questions
Patient	Should the hospital take the patients' privacy preferences into account? Or is it enough that the patients just give their consent? How much details (if any) should be provided to the patients (w.r.t how their data is being processed)? How should the patients be informed (and compensated) if their data have been compromised?
Hospital	How can the hospital ensure that the patients' data are processed in accordance to the agreed terms (cf. the contract between the hospital and the cloud service providers)? How can the hospital make sure that the processing of the patients' data is compliant with legislation? What source of information can the hospital use to assess the trustworthiness of the cloud service providers they engage? How will the hospital be affected if the patients' data are compromised?
Provider	How can the cloud service providers make their service more trustworthy to potential customers in the health care domain? How can the cloud service providers be more transparent (w.r.t how they process the patients' data)? What should be expected from the cloud service providers if the patients' data are compromised?
Regulator	How can cloud service providers make their services more trustworthy to potential clients in the health domain? How can cloud service providers become more transparent (in terms of how they process the patients' data)? What should one might expect from cloud service providers if patient data compromised?
Open discussion	Here the participants could choose which topics they would like to discuss (related to the healthcare scenario).

TABLE I: Discussion questions for the focus groups.

Session (time)	Patient	Hospital	Provider	Regulator	Open discussions
19:20-19:40	2	12	6	7	2
19:45-20:05	12	6	8	5	0
20:10-20:30	3	0	0	0	2

TABLE II: The number of participants in the different focus group sessions.

X or Y. The information engine, which visualizes and displays information to the end users, will be implemented in M's own infrastructure (Cloud z). As can be seen in Fig. 1, through graphical user interfaces (GUIs) the platform will interact with and provide services to a number of different users involved. Data that are being stored or processed in Cloud x or Cloud y are only accessible through using Cloud z, which provides GUIs for patients, relatives and friends, as well as selected employees (physicians and caregivers) at the hospital. Note that it is the hospital that provides accounts and logins to patients, relatives, staff etc., to enable them to access data through Cloud z.

Our previous experiences with stakeholders in the healthcare sector tell us that they usually pay close attention to regulations and compliance when they discuss emerging technologies. During the presentation of the "M Platform", the first author of this paper therefore gave a brief introduction to the responsibilities of the involved actors in the M Platform service delivery, which was based on European data protection law. In short, it was explained that, according to Directive 95/46/EC [3], which in Norway has been implemented in national legislation as the Personal Data Act 2000 [16], healthcare data are classified as *sensitive personal data* and that it is the hospital who is accountable to the patients for the processing of their personal data, even though the actual collection, storage and further processing tasks have been outsourced to third party service providers (provider X, Y and Z). We also explain that, according to Directive 95/46/EC, none of the involved third party service providers are directly accountable to the patients, but would be accountable to the hospital under the terms of the contracts that must exist between them and the hospital[2].

IV. Obstacles to Adoption

In this section we present the main obstacles to adoption of a cloud-based solution like the M Platform, which were raised and discussed by the stakeholders during the open space session.

> *"I believe it is more secure to store health care data in a cloud rather than on the PC in a medical office, without backup."* - A stakeholder expressing his opinion at the open space session.

Ownership. Ownership to patient data was pointed out as an obstacle by several of the stakeholders. They seemingly agreed that the patients are the owners of their personal data that are collected and processed in a healthcare application like the M Platform. However, they pointed out that the fact that the patients own their healthcare data seemed to be difficult to accept by the healthcare personnel, who regularly claim access to patient data. A situation was mentioned, where doctors using an application that only allowed on-screen viewing of patient data still would copy screenshots from particularly interesting cases to their personal memory sticks, in order to keep them for future reference.

Privacy preferences. Most of the stakeholders agreed that when personal data are collected from patients, the patients' privacy preferences should be taken into account. However,

[2]A further discussion of the allocation of responsibilities between the involved actors in this use case, under the existing data protection law, is provided by Bernsmed et al. [17].

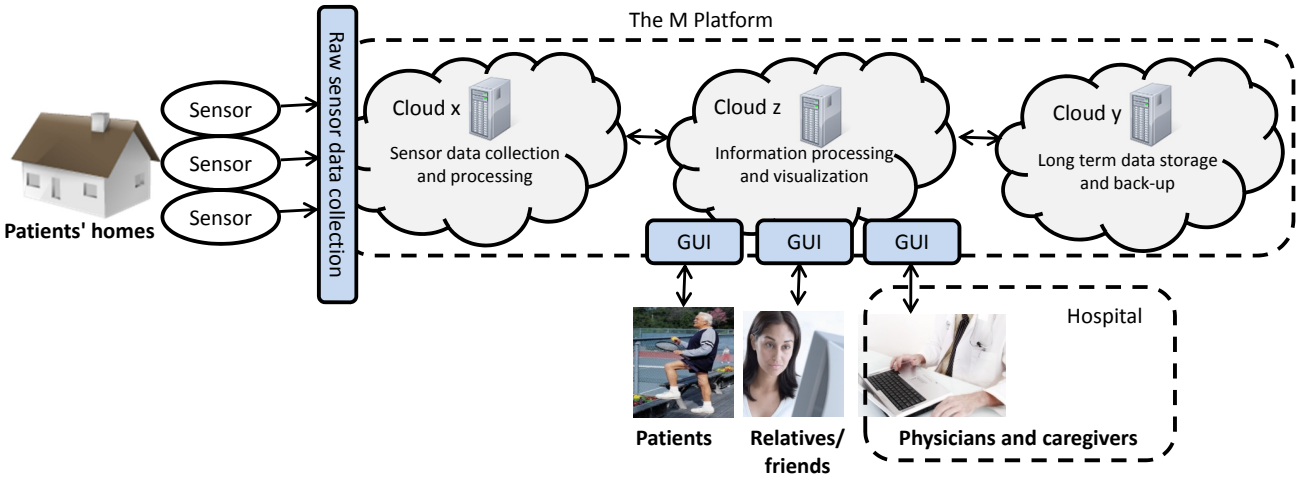

Fig. 1: An overview of the "M Platform', which was used as input to the discussions in the open space session.

the stakeholders also pointed out that being able to access the required (personal) health information at any time is a must for health care personnel, and that their healthcare data is available is also required and desired by (most of) the patients. There is hence a conflict between availability and privacy, but from the patient perspective, availability is the main priority, the stakeholders maintained.

Putting the patients in control. In a scenario like the one outlined in Fig. 1, large amounts of (sensitive) personal data will be collected from the patients. In the proposed solution the definition of appropriate policies to govern the use of personal data processing will be done through an administration interface in the M Platform. However, one of the stakeholders strongly argued that the patients should be given more control. Rather than administrating the personal data policies through Cloud Z, the patients should be able to configure the sensors' data collection capabilities directly by themselves, thereby being able to directly prevent unwanted data collection. However, another stakeholder pointed out that this would make the solution much more complex (and probably more expensive). A third stakeholder further argued that patients cannot be expected to understand how to configure the sensors and that it is the hospital's responsibility to make sure that personal data is only collected in accordance with the patients' preferences. The degree to what the patients should be given control was clearly a topic where the stakeholders had different views and opinions.

The quality of the sensors. The introduction of "Diagnose-It-Yourself" sensors in the private consumer market raised a lively discussion amongst the stakeholders.

> *"Going to bed with an app [to measure sleep quality]? No, thank you! This can never provide data having nearly the same quality as professional medical equipment."*

However, another stakeholder stated that measurements that are recorded close to, e.g., a cardiac infarction are worth a lot. Here there is a conflict with private medical equipment that might not be accurate or calibrated correctly, since there is always a trade-off between time and quality. Can we afford to refuse all such data if the medical professional cannot rely 100% on their quality? The stakeholders did not have a clear answer to this question. However, they stated that quality of, and hence confidence in, medical data is essential for medical appliances, and that private sources of such data are very difficult to make use of in practice. One stakeholder pointed out that they (speaking from the service provider's point of view) did not consider sensor data from other sources than the hospital as reliable, and could probably not see the practical use of the data.

The lack of evidence. In the introductory presentation of the use case it was explained that, according to European data protection law, it is the hospital's responsibility to make sure that personal data is fairly and lawfully processed in a cloud-based solution such as the M Platform, and the hospital therefore needs to make sure that the cloud providers' data processing practices are compliant with existing legislation. The stakeholders therefore discussed some issues that should be included into contracts to assure that relevant legislations and regulations are being met. However, several of the stakeholders pointed out that even though the hospital's contract with the M Platform provider is water-tight, there is little the hospital can do to ensure that the promises in the contract are being fulfilled, and that this lack of evidence is a major problem.

Informal information sharing. Back in the days, before the electronic healthcare records were introduced, hospital staff that arrived at work would be notified by the leaving staff that "OK, this patient is a bit grumpy today, handle him like this and this", or they would have small yellow

stickers placed on their desks. Information necessary to keep the flow going was not always appropriate for the formal patient record, but would rather be communicated in short informal meetings (paradoxically, often involving tobacco in one form or another). Nowadays, with the introduction of electronic patient records, it is difficult for healthcare personnel to know how and where in the records this kind of informal information should be entered, or even if it should be documented at all. The stakeholders also mentioned that healthcare personnel with little technical knowledge seem to be particularly reluctant about entering informal data in the patients' records. Some of the stakeholders believed that this problem would become even more apparent with the adoption of cloud technology.

Audit logs. The stakeholders also mentioned that when new IT systems are considered for purchase, their audit log capabilities is a very important factor. Who has accessed patient X's record? Which records has employee Y been looking at? They stated that this kind of information needs to be registered and securely saved for future reference. They also pointed out that in a solution like the M Platform, not only the employees at the hospital but also the employees at the different cloud service providers may have access to patient data and their accesses therefore also need to be audited and logged.

On-site audits. The possibilities to do on-site audits at the cloud service providers' premises were also discussed and the stakeholders expressed frustration regarding the difficulties for small players to demand any kind of audit rights from the big cloud service providers. They discussed the current situation in Norway, where most of the hospitals and health care organisations are small entities with limited possibilities to make demands and stated that small entities should be able to join forces in order to have a bigger impact (however they disagreed about whether this would work in practice). As an example one of the stakeholders stated that 200 small hospitals who use (e.g.) Azure cannot individually walk up to Microsoft and demand to perform an audit, but serious players perform regular third party audits that customers can demand access to.

The role of the Norwegian Data Protection Authority (DPA) in the audit process was also briefly discussed. One stakeholder stated that the DPA will never go after a foreign cloud provider, but rather focus on for example municipalities or hospitals that have used the cloud in an "unsafe" (non-compliant) way. He also pointed out that the DPA only do spot checks; they cannot and will not audit every municipality or health care organisation in the country.

Standardization. The stakeholders experience the lack of good standards for cloud-based healthcare application as a major problem. From the buyer's perspective, healthcare organisations always prefer standardized solutions and they expect that the suppliers adhere to these. Likewise, suppliers also support standardization, as this makes it easier to navigate the domain and to know what their customers expect. Right now it is very difficult to know to what degree they can or cannot integrate cloud services in their health care solutions.

The risk of centralization. Today, in Norway all healthcare organisations and hospitals manage their own IT systems and all their patient data is stored locally in their own servers. The stakeholders pointed out that there is an advantage with the existing approach; if there is a data breach in one hospital it will therefore only affect a limited number of patients. They considered this to be a good thing, and pointed out that the differences between the consequences of data breaches in big cloud datacenters and the break-down of for example one doctor's laptop.

Legal obstacles. Finally, the legal aspects of outsourcing personal data (and healthcare data in particular) to the cloud was considered to be a main obstacle, according to the stakeholders. Their discussions revealed that data protection legislations is perceived as an almost insurmountable barrier to the adoption of public cloud services. They also discussed the Norwegian archival legislation, which require that at least one copy of all public records in Norway (including healthcare records) are stored in Norway. Legal obstacles hence seemed to be a major concern to the adoption of cloud services in the healthcare domain.

V. Discussion

Our main impression from the stakeholders' discussions is that availability is a key requirement for healthcare applications. Clearly the participants were more concerned with data as a "transparent thing" that should just be around, and that availability is the ultimate goal. Whether or not hospitals and other healthcare organisations in Norway could use cloud services or not did not seem to be the question, perhaps because they did not seem to comprehend the term "cloud" as something very different from a centralized collection of patient records; i.e., something that can be easily accessed from many places, compared with the situation today where healthcare data from different regions often are physically separated. As shown in Table III, these findings are consistent with previous literature [18], [10], [11]. In the study by Rodrigues et al. [11] they state that cloud service providers' customers should be informed about the services the cloud provider offers them and the security mechanisms installed on the provider's servers. Cloud users should demand total transparency from the cloud service provider.

Any cloud-based solution will most likely introduce more than one new player in the service delivery chain (as illustrated in Fig. 1, services are often outsourced to third parties who in turn outsource parts of their services to other parties) and, from the hospital's point of view, this may decrease their transparency with respect to what happens to the patients' data. This makes it more difficult for the hospitals to ensure that their health care systems and applications are compliant with

existing legislation. The stakeholders all seemed to be aware of this problem and it seemed like they considered this to be one of the main obstacles to adoption of public cloud services. It should be noted that these focus group sessions focused on the processing of (sensitive) personal data in the cloud, and even though there is a large body of other legislation that applies to the processing of healthcare data, being compliant with the data protection legislation still seemed to be the most significant barrier against the adoption of cloud-based services in healthcare. Legal aspects have also been listed as challenges in other studies as shown in Table III. This is further supported by Rodrigues et al. [11], who state that a legal framework must guide the policies of the cloud provider. Also Liu and Park [18] state that one of the greatest challenges for organizations leveraging cloud environments is demonstrating policy compliance.

Another interesting aspect of the stakeholders' discussions was their emphasis on the necessity of access control and audit logs to the healthcare data. Existing IT solutions often come with strong access control mechanisms (that thoroughly log which user has accessed what data and when), but in practice this is often circumvented in the hospitals as doctors regularly log in when they arrive to work in the morning and leave their accounts open throughout the day for any of the other healthcare personnel to access. This underpins our understanding of availability of patient data as being the main priority for healthcare personnel, but at the same time it undermines any possibility of logging who has accessed the patient data and when. Clearly there is a need for better, and other types of, access control mechanisms that are seamlessly integrated and workable in practice in the day-to-day tasks at the hospital. AbuKhousa et al. [10] and Rodrigues et al. [11] discuss the need to demonstrate readiness for external audits. Rodrigues et al. [11] further state that for maintaining the security and privacy of an electronic health record (EHR), when it comes to audits, an audit register should include all accesses to the information and all the changes that have taken place to the EHRs.

Previous work has identified the other challenges associated with the cloud and healthcare. Table III summarizes the main challenges described in the literature.

VI. Accountability as a Way Forward

Accountability is a fairly recent concept in the world of computer networking, and often not easily understood or even properly defined. For our purposes, the definition provided by the Galway project [21] provides a useful starting point:

> "An accountability-based approach requires that organizations that collect, process or otherwise use personal information take responsibility for its protection and appropriate use beyond mere legal requirements, and that they be accountable for any misuse of the information that is in their care." [21]

Accountability is likely to become a core concept in both the cloud and in new mechanisms that help increase trust in cloud computing [22]. These mechanisms must be applied in an intelligent way, taking context into account and avoiding a one-size-fits-all approach. Pearson [22] argues that an accountability-based approach requires organizations to:

- commit to accountability and establish policies consistent with recognized external criteria;
- provide transparency and mechanisms for individual participation, including sharing these policies with stakeholders and soliciting feedback;
- use preemptive approaches (to assess risk and avoid privacy harm) and reactive approaches (that provide transparency and auditing) to implement these policies, including clear documentation and communication (encompassing an organization's ethical code), support from all levels within the organizational structure, tools, training, education, ongoing analysis, and updating;
- allow validation that is, provide means for external enforcement, monitoring, and auditing; and
- provide mechanisms for remediation, which should include event management (such as dealing with data breaches) and complaint handling.

Our findings indicate that, in the healthcare domain, stakeholders are concerned with availability, transparency, compliance with data protection legislation, access control and audit logs. An accountability-based approach will help mitigate all of these concerns. By providing transparency and audit logs, individuals will be adequately informed by the cloud providers about how their data are processed in the cloud, and the division of responsibilities between the involved organizations will become clear. Transparency in cloud computing is important; not only for legal and regulatory reasons, but also to avoid violation of social norms [23]. The corporate user provides assurance and transparency to the customer/client through its privacy policy, while requiring similar assurances from the service provider through contractual measures and audits.

Accountability will help ensuring that the cloud service complies with laws, and also challenges that are related to organisational policies can be tackled [24], [25]. Today, to be compliant with data protection laws and regulations, it is often necessary for cloud customers to require that the data processing take place in a certain geographic location. If cloud services providers become accountable, location may become less relevant to the customers, because they can be assured by other means that their data will be treated as promised regardless of what jurisdiction applies. Also the actual data processing will become much more transparent through contracts specifying where data processing will take place [24]. Today, the stakeholders that participated in our study did not even consider location to be an obstacle; they seemed to implcitly assume that processing healthcare data in another country will never be allowed.

Still, one might ask "Why would a provider stick its neck out beyond what is required by law?" Clearly, few (if any) cloud providers in the current landscape can offer the level of accountability stakeholders in the (European) healthcare sector are looking for. As accountable providers emerge, cloud

Aspects	Opportunities	Challenges
Management	• Lower cost of new IT infrastructure [8] • Computing resources available on demand [8] • Payment of use on a short-term basis as needed [8]	• Lack of trust by health care professionals [8], [19] • Organizational inertia [8], [9] • Loss of governance [8], [9] • Ease of access and flexible configuration for the users [18], [10] • Uncertain provider's compliance [8], [9] • Uncertain provider reputation [11] • Unknown Risk Profile [20] • Providers Demonstrate Transparency [11]
Technology	• Reduction of IT maintenance burdens [8] • Scalability and flexibility of infrastructure [8] • Advantage for green computing [8]	• Resource exhaustion issues [8], [9] • Unpredictable performance [8], [9], [19] • Reliability and Availability [10] • Data lock-in [8] • Data transfer bottlenecks [8], [9] • Bugs in large-scale distributed cloud systems [8], [9], [10] • Organizational Inertia [9] • Data and Systems Interoperability [18], [12], [19], [10] • Shared Technology [20] • Data Location [11] • Data Logging and Monitoring [11], [10] • Scalability and flexibility of infrastructure [10]
Security	• More resources available for data protection [8] • Replication of data in multiple locations increasing data security [8] • Dynamically scaled defensive resources strengthening resilience [8]	• Separation failure [8], [9], [11], [19] • Public management interface issues [8], [9] • Poor encryption key management [8], [9] • Privilege abuse [8], [9], [10] • Abuse and nefarious use of the cloud [18], [20], [10] • Malicious insiders [18], [20], [11], [19], [10] • Insecure interfaces and APIs [18], [20] • Account or service hijacking [18], [20], [10] • Data Loss or Leakage [18], [12], [10] • Ensuring the accuracy and consistency of data [10] • Non-repudiation [10]
Legal	• Provider's commitments to protect customer's data and privacy [8] • Development of guidelines and technologies to enable the construction of trusted platforms by not-for-profit organizations [8] • Fostering of regulations by government for data and privacy protection [8]	• Data jurisdiction issues [8], [9], [11], [19] • Privacy issues [8], [9], [12], [11], [10] • Trust and Liability issues [10] • Demonstrating policy compliance [18], [11] • Demonstrate readiness for external audits [11], [10] • Guarantee continuity of service in case of problems [11] • Data ownership [10]

TABLE III: Opportunities and Challenges for Cloud Computing in eHealth

users will need tools that help them select providers that can fulfill their accountability requirements. In our example, the hospital would use a tool for data protection impact assessment to identify the risk and threats associated with the processing of sensitive personal data in the cloud, and an advisory tool to identify a provider that offers a sufficient level of transparency, and that can document their data handling practices. The inherent challenge in cloud computing is that it is not sufficient that the provider with whom you have a contract is accountable; all the other providers in the provider chain must be accountable too. The clue to achieving this is to provide mechanisms that automatically can traverse the service delivery chain; transferring the required information in each step.

The Eu FP7 A4Cloud project is an ongoing research project[3], which aims to increase the adoption of cloud technology in, for example, the healthcare domain. Our approach is based on the premise that creating a completely secure technical solution (independent of your definition of "secure") is not possible. Realising the difficulties of preventing cloud providers from doing unsavoury things with data that are being stored in their data centers, we claim that the next best thing is to introduce procedures, mechanisms, and tools that enable cloud providers to be accountable to their users. At the same time, potential cloud customers should be empowered to make informed choices about selection of a service provider based on a solid understanding of the consequences of its choices.

[3]http://www.a4cloud.eu/

VII. Conclusions

Cloud computing has been receiving a great deal of attention, both in the academic field and amongst the users of IT services, from individuals at hospitals, to medical offices and to the government. The results from our focus groups show

that stakeholders in the healthcare domain consider uncertainties with respect to data ownership, the conflict between patient privacy and availability of medical data, the lack of evidence of the providers' data processing practices, the difficulties to do on-site audits, and possible problems with compliance, to be major obstacles for the processing of healthcare data in the cloud. Our work hence reaffirms the results of previous studies.

Many of the challenges that we have identified can be addressed by increasing the accountability of cloud service providers. Our contention is that being accountable can be a business advantage, and that cloud customers who are concerned with, e.g., privacy of the data they put into the cloud, will choose providers who can demonstrate accountability over providers who cannot.

ACKNOWLEDGEMENTS

This work has been partly funded from the European Commissions Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD) Cloud Accountability Project[3] .

REFERENCES

[1] J. Ko, C. Lu, M. Srivastava, J. Stankovic, A. Terzis, and M. Welsh, "Wireless Sensor Networks for Healthcare," *Proceedings of the IEEE*, vol. 98, no. 11, pp. 1947–1960, 2010.

[2] J. Biswas, J. Maniyeri, K. Gopalakrishnan, L. Shue, P. Eugene, H. Palit, F. Y. Siang, L. L. Seng, and L. Xiaorong, "Processing of wearable sensor data on the cloud - a step towards scaling of continuous monitoring of health and well-being," in *Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE*, 2010, pp. 3860–3863.

[3] European Parliament, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data." pp. 31–50, 1995. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[4] K. Bernsmed, M. Felici, A. S. D. Oliveira, J. Sendor, N. B. Moe, T. Rübsamen, V. Tountopoulos, and B. Hasnain, "Use case descriptions," Cloud Accountability (A4Cloud) Project, Deliverable, 2013.

[5] I. R. Kabashiki, "Cloud Computing and Healthcare Delivery in Canada: An exploratory Investigation," *Journal of Leadership and Organizational Effectiveness*, vol. 1, no. 4, pp. 4–17, 2013.

[6] N. Sultan, "Making use of cloud computing for healthcare provision: Opportunities and challenges," *International Journal of Information Management*, vol. 34, no. 2, pp. 177 – 184, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0268401213001680

[7] J.-W. Lian, D. C. Yen, and Y.-T. Wang, "An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in taiwan hospital," *International Journal of Information Management*, vol. 34, no. 1, pp. 28 – 36, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0268401213001138

[8] A. M.-H. Kuo, "Opportunities and challenges of cloud computing to improve health care services," *J. Med. Internet Res.*, vol. 13, no. 3, p. e67, 2011. [Online]. Available: http://dx.doi.org/10.2196/jmir.1867

[9] G. Gavrilov and V. Trajkovik, "Security and privacy issues and requirements for healthcare cloud computing," in *Proceedings of ICT Innovations*, 2012. [Online]. Available: http://ictinnovations.org/2012/htmls/papers/icti2012_submission_16.pdf

[10] E. AbuKhousa, N. Mohamed, and J. Al-Jaroodi, "e-health cloud: Opportunities and challenges," *Future Internet*, vol. 4, no. 3, pp. 621–645, 2012. [Online]. Available: http://www.mdpi.com/1999-5903/4/3/621

[11] J. J. Rodrigues, I. de la Torre, G. Fernandez, and M. Lopez-Coronado, "Analysis of the security and privacy requirements of cloud-based electronic health records systems," *J. Med. Internet Res.*, vol. 15, no. 8, p. e186, 2013. [Online]. Available: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3757992/

[12] S. P. Ahuja, S. Mani, and J. Zambrano, "A Survey of the State of Cloud Computing in Healthcare," *Network and Communication Technologies*, vol. 1, no. 2, p. 12, 2012. [Online]. Available: http://www.ccsenet.org/journal/index.php/nct/article/view/19240

[13] R. A. Krueger, *Focus Groups: A Practical Guide for Applied Research*. SAGE Publications, 1988.

[14] D. W. Stewart, *Focus groups: Theory and practice*. Sage, 2007, vol. 20.

[15] M. Daneva and N. Ahituv, "Evaluating cross-organizational erp requirements engineering practices: a focus group study," in *Research Challenges in Information Science (RCIS), 2010 Fourth International Conference on*, May 2010, pp. 279–286.

[16] "Act of 14 april 2000 no. 31 relating to the processing of personal data (personal data act)." [Online]. Available: http://www.datatilsynet.no/Global/english/Personal_Data_Act_20120420.pdf

[17] K. Bernsmed, W. K. Hon, and C. Millard, "Deploying Medical Sensor Networks in the Cloud Accountability Obligations from a European Perspective," in *Proceedings of the 7th IEEE International Conference on Cloud Computing (IEEE CLOUD 2014)*, 2014.

[18] W. Liu and E. Park, "e-healthcare cloud computing application solutions: Cloud-enabling characteristices, challenges and adaptations," in *Computing, Networking and Communications (ICNC), 2013 International Conference on*, Jan 2013, pp. 437–443.

[19] M.-H. Kuo, "A healthcare cloud computing strategic planning model," in *Computer Science and Convergence*, ser. Lecture Notes in Electrical Engineering, J. J. (Jong Hyuk) Park, H.-C. Chao, M. S. Obaidat, and J. Kim, Eds. Springer Netherlands, 2012, vol. 114, pp. 769–775. [Online]. Available: http://dx.doi.org/10.1007/978-94-007-2792-2_76

[20] "Top Threats to to Cloud Computing Report (Ver.1.0)," Cloud Security Alliance, 2010. [Online]. Available: http://cloudsecurityalliance.org

[21] Galway Project, "Data protection accountability: The essential elements a document for discussion," October 2009, http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf.

[22] S. Pearson, "Toward accountability in the cloud," *Internet Computing, IEEE*, vol. 15, no. 4, pp. 64–69, July 2011.

[23] K. Khadke and P. U. Chavan, "Survey on distributed accountability for data sharing in the cloud," *International Journal of Computer Science and Mobile Computing - IJCSMC*, vol. 3, no. 1, January 2014.

[24] S. Pearson and A. Charlesworth, "Accountability as a way forward for privacy protection in the cloud," in *Proceedings of the 1st International Conference on Cloud Computing*, ser. CloudCom '09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 131–144. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-10665-1_12

[25] P. T. Jaeger, J. Lin, and J. M. Grimes, "Cloud computing and information policy: Computing in a policy cloud?" *Journal of Information Technology amp; Politics*, vol. 5, no. 3, pp. 269–283, 2008. [Online]. Available: http://dx.doi.org/10.1080/19331680802425479