2020 IEEE International Conference on E-health Networking, Application & Services (HEALTHCOM) | 978-1-7281-6267-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/HEALTHCOM49281.2021.9399006

Healthcare and data privacy requirements for e-health cloud: a qualitative analysis of clinician perspectives

Taridzo Chomutare[1,*], Kassaye Yitbarek Yigzaw[1,*], Silvia Delgado Olabarriaga[2], Alexandra Makhlysheva[1], Marcela Tuler de Oliveira[2], Line Silsand[1], Dagmar Krefting[3,5], Thomas Penzel[4], Christiaan Hillen[6], and Johan Gustav Bellika[1,7]

[1]Norwegian Centre for E-health Research, Tromsø, Norway
[2]University of Amsterdam, Amsterdam, The Netherlands
[3]HTW Berlin - University of Applied Sciences, Berlin, Germany
[4]Charité – Universitätsmedizin Berlin, Berlin, Germany
[5]University Medical Center of Göttingen, Göttingen, Germany
[6]Secura, Eindhoven, The Netherlands
[7]UiT The Arctic University of Norway, Tromsø, Norway
[*]These authors contributed equally

***Abstract*—Cloud computing has many benefits relevant to the healthcare industry. Although the adoption of cloud services for healthcare systems is increasing, employment of cloud services raises many security and privacy concerns for patients and healthcare providers. We still lack a clear set of requirements consented by the different stakeholders; here in particular IT and healthcare professionals. In this study, we examine whether user perspectives on requirements for e-health on the cloud are consistent with best practice guidelines and regulatory requirements. This work contributes to the requirements engineering phase for a secure e-health cloud framework developed in a European project (ASCLEPIOS, https://www.asclepios-project.eu/). We used qualitative analysis, based on in-depth interviews, to describe and characterize clinicians' perspectives on the requirements of cloud services for healthcare data security and privacy. We examined whether these user perspectives were in harmony with the regulatory framework of the General Data Protection Regulation (GDPR), and best practice guidelines of a relevant standard, ISO 18308:2011. Ten clinicians were identified and interviewed at six healthcare organizations in Norway, the Netherlands and Germany. While user perspectives were largely consistent with both GDPR and ISO, some concerning differences in access control were noted between large and small healthcare institutions.**

***Index Terms*—Cloud, eHealth, requirements, qualitative**

I. Introduction

Cloud computing generally refers to the on-demand use of data storage and computing resources as a service offered over the internet, without direct management of these services by the user. As formally defined by the National Institute of Standards and Technology (NIST) [1], 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."

From NIST's four deployment models, the two core delivery models for cloud services are the private and public clouds. A private cloud is provisioned for use by a single organization and the servers might be physically located at that organization. A public cloud exists on the premises of the cloud service provider (CSP) and may be used by any of its customers, simultaneously. In most cases, the public cloud is what is assumed when discussing cloud services although actual implementations vary. Discussion in the context of this study focuses on the public cloud paradigm since it is the most flexible and cost-effective, but also presents the most challenges regarding the security and privacy of data processing in the healthcare setting.

Cloud services have emerged as an essential solution for modern computing and have become a significant area of interest in healthcare because of their flexibility, ease of access, and service levels. Traditionally, computer systems in healthcare have been localized, but recent trends in electronic health record (EHR) systems adoption have heightened the need for more robust computing and collaborative platforms. The key benefit of cloud computing is a more efficient provision of computing power, storage and networking resources. For the healthcare sector, these benefit impact both the economic and information management perspectives [2]. These include, lower upfront costs for the deployment of complex computer systems such as EHRs, lower costs for maintaining systems, and ubiquitous access to these resources via the internet.

Despite these benefits, some of the primary concerns and

This work was supported by the European Commission's H2020 research and innovation programme Project No. 826093; "Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare" (ASCLEPIOS). The funding body did not have any role in the study and writing of the manuscript.

often the most frequently cited problems with cloud computing for healthcare are data protection and privacy [3]. In a recent review, Al-Issa et al. [4] summarized two sources of major concern. First, even if the actual data stores are physically distributed, the data is still centralized within the CSP, making this a high-value target for hackers, as well as for malicious insiders. Second, using the services of a CSP may lead to the understanding that data ownership is also shifted to that CSP. This gives rise to the impression of less control over the data by the healthcare institution. Potential conflicts between new computing paradigms such as cloud computing and regulations on data concerning health are a well-known problem [5].

Previously, there were no specific regulations or standards to guide the development of cloud services in healthcare [6], [7], but today there are internationally agreed regulations and standards, such as the GDPR and ISO standards. However, there is still a lack of an encompassing framework that reconciles all the current guidelines as well as user perspectives. So far, the research on requirements for cloud computing in healthcare is mostly descriptive and based on narrative reviews. Moreover, no studies have examined whether the perceptions of healthcare professionals are in line with current regulations and best practice.

This study aims to investigate in what ways user perspectives on requirements for e-health cloud services are in harmony or conflict with the requirements of the GDPR and best practice guidelines of the ISO 18308:2011 standard. To answer this question, we used a qualitative approach based on interviews already conducted in the broader scope of the European project "Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare" [8]. The goal of the project is to build a cloud-based e-health framework that safeguards data concerning health from internal and external attacks, and protect the privacy of data subjects.

II. Methods

A. Study design

We used a qualitative approach based on a series of local knowledge cases, in three different European countries (Norway, the Netherlands and Germany), to describe and characterize clinician perspectives on healthcare and data privacy requirements for cloud services. We used an inductive approach, working from the ground up to gather in-depth perspectives that were not driven by technically proficient experts, but non-technical user viewpoints.

Purposeful sampling was used to identify clinicians at healthcare institutions in the three countries. Co-authors in the three countries identified key persons at health institutions in their respective countries. We coordinated the sampling to include both large institutions like regional hospitals and smaller health institutions like general practitioner (GP) offices.

B. Data collection

A panel of experts developed the questionnaire (see Appendix 1) used as an interview guide. The panel of experts comprised technical experts in health data security and privacy-preserving methods for processing health data. The panel also included experts with clinical backgrounds. The interview guide was developed iteratively, assessed for completeness and accuracy, and a test evaluation run was performed with a clinician before the actual interviews were conducted. In-depth semi-structured interviews were conducted, and audio was recorded during the interview. Each interview lasted around one hour. The interviewers generated a pseudonymized transcript of each interview from which all the identifying information was removed. Then, a unique code was assigned to the transcript and the audio record. All the transcripts were stored in a secure storage device with restricted access to the project members who were listed on the consent form. However, access to the audio records were limited to project members who conducted the interviews.

C. Ethics

All participants gave their consent before the interviews. Since the interviews were conducted in the broader scope of the European project ASCLEPIOS, the study design and informed consent forms were assessed by the ethics committee and data protection officer of the ASCLEPIOS project. They concluded that more rigorous ethical review was not necessary because the study did not collect sensitive information. Encrypted audio records were locally maintained in each of the three countries, and only the pseudonymized transcripts were shared with other project members who were involved in the study. The audio records will be retained until the end of the project in 2021, and the transcripts will be retained five years after the end of the project.

D. Content analysis and coding

Two co-authors coded the transcripts, and some of the other co-authors verified the themes and codes. The codes were generated in two ways; first, from the keywords and trigger words pre-defined in the interview guide, and second, from the iterative review of the transcripts. To generate codes from the transcripts, we iteratively tagged keywords and phrases that summarize every sentence in each response. Each response could be comprised of several keywords, which were then categorized into one or more themes. The themes were used to determine the code. Table I illustrates an example of the coding process based on the interview question regarding how the participants understood or viewed cloud services, and what the possible benefits were. Some of the codes that emerged from that discussion were: remote computing resource (CR), ubiquitous CR, scalable CR, low cost and security.

E. Comparison with GDPR and ISO 18308:2011

The analyzed content from the interviews is described in light of regulatory guidelines and best practices relevant to management of medical data. Medical data include reports, findings, letters, medical image data and medical signal data in this context. Comparison with the GDPR is meant to highlight any apparent conflicts between participants' perceptions and

TABLE I
AN EXAMPLE OF A CODING DISCUSSION ON PARTICIPANTS' UNDERSTANDING OF CLOUD SERVICES

Transcription with keywords and phrases	Code
"It can be **cheaper**."	Low cost
"**Reduced IT costs** and staff and **better information security** because safeguarding security should part of the core business of cloud provider."	Low cost, Security
"**Better availability**; **efficient** and **secure data sharing**"	Availability, Security
"**IT technology** with machines in the houses **somewhere in the world**"	Remote CR
"Internet-based **software, applications and services** provided by providers to **share data** - or to **access to applications from another place**. The user has **access through the internet** and often has to pay for it. Mostly protected by an institutional firewall."	Remote CR, Ubiquitous CR

the requirements of the regulation. The goal was not to identify missing GDPR aspects, but rather to examine if the aspects raised in the interviews were in harmony with the GDPR.

The themes and codes extracted from the interview transcripts were compared to the following chapters of the GDPR: (i) rights of the data subject (chap.3), (ii) controller and processor (chap.4), and (iii) transfer of personal data to third countries or international organizations (chap.5).

In terms of the the ISO standard, we used the ISO 18308:2011 standard titled "Health informatics — Requirements for an electronic health record architecture" as it describes functional requirements and architectural specifications for EHRs. Again, the extracted themes and codes were compared to two main chapters of the ISO standard: (i) EHR business objectives (chap.5), and (ii) requirements for an EHR architecture (chap.6). These two chapters contain wide ranging topics such as health system objectives, citizen inclusion objectives and ethical and legal requirements.

F. Differences between countries and institution type

Additionally, we assessed perceptions per country, since different countries have different contexts regarding regulations for managing healthcare systems. Healthcare professionals must work within these regulations and limitations, and this may influence their view of requirements and needs. This analysis also takes into account the size of the institution.

III. RESULTS

A. Characteristics of participants and their institutions

Ten interviews were conducted at six healthcare institutions comprising three hospitals, two GP offices, and one university hospital (department for sleep medicine). All the participants were clinicians (n=10). Most of the participants self-rated their awareness of GDPR requirements as above average (7/10), while the rest indicated average awareness (2/10) or below-average awareness (1/10).

Half of the institutions involved are large, with more than five thousand employees, and the other half have less than 20 employees. These health institutions are located in three European countries: Norway, the Netherlands and Germany. In terms of IT support, two institutions had in-house support, three outsourced support, and one had both in-house and outsourced support.

Turning to clinician perspectives, the four main themes; (i) perceived benefits and concerns regarding public cloud services, (ii) data access control, (iii) service availability, integrity and transparency, and (iv) data reuse, and seventy-three codes arising from the interviews are summarised in Fig. 1 Each of the themes is discussed in more detail below.

B. Perceived benefits and concerns about public cloud

All the institutions had their EHR and other health data on their premises on a private cloud. One reason for not using public cloud services was security concerns, and some participants also pointed out that they did not see the benefit of a public cloud since they used a private cloud. Moreover, some clinicians were not aware of how the decisions regarding public cloud services were made.

Participants were able to point out the essential characteristics of a cloud service: it is a computing resource, and it is remote. Another critical aspect of the cloud that was mentioned in the interviews was service provisioning in a ubiquitous manner through connected mobile devices. Moreover, some of the key benefits of cloud services were named, such as ease of data access, data sharing and backup, the potential to lower costs, faster to deploy services, scalability and higher availability.

One of the cited concerns was the lack of control of public cloud services since the cloud service provider would not be a part of the health institution. Some participants questioned trust in cloud service providers and whether the providers would be able to comply with the data protection laws.

> *"The biggest fear is obviously that someone who is not allowed to could access the data."*

C. Perspectives on access control

Currently, clinicians across the institutions have access to all data about their patients if stored on central databases and repositories. They also have full access to data about individuals who are not their patients in cases of emergency. In this case, the clinician must explain the reason for the access. In some institutions, health professionals only have access to the part of the record that is necessary for their job. In some systems, patients do not have the power to control access to their records, but they may request access to a record entry to be restricted. A distinction should be made between larger institutions and smaller GP offices: in the latter, the clinicians have typically unrestricted access to the EHR and all patients in the practice.

Role-based access control to the EHR was mentioned in the interviews, and also that the access should be kept secure and traceable. However, the participants were generally satisfied with the current access control techniques and expressed

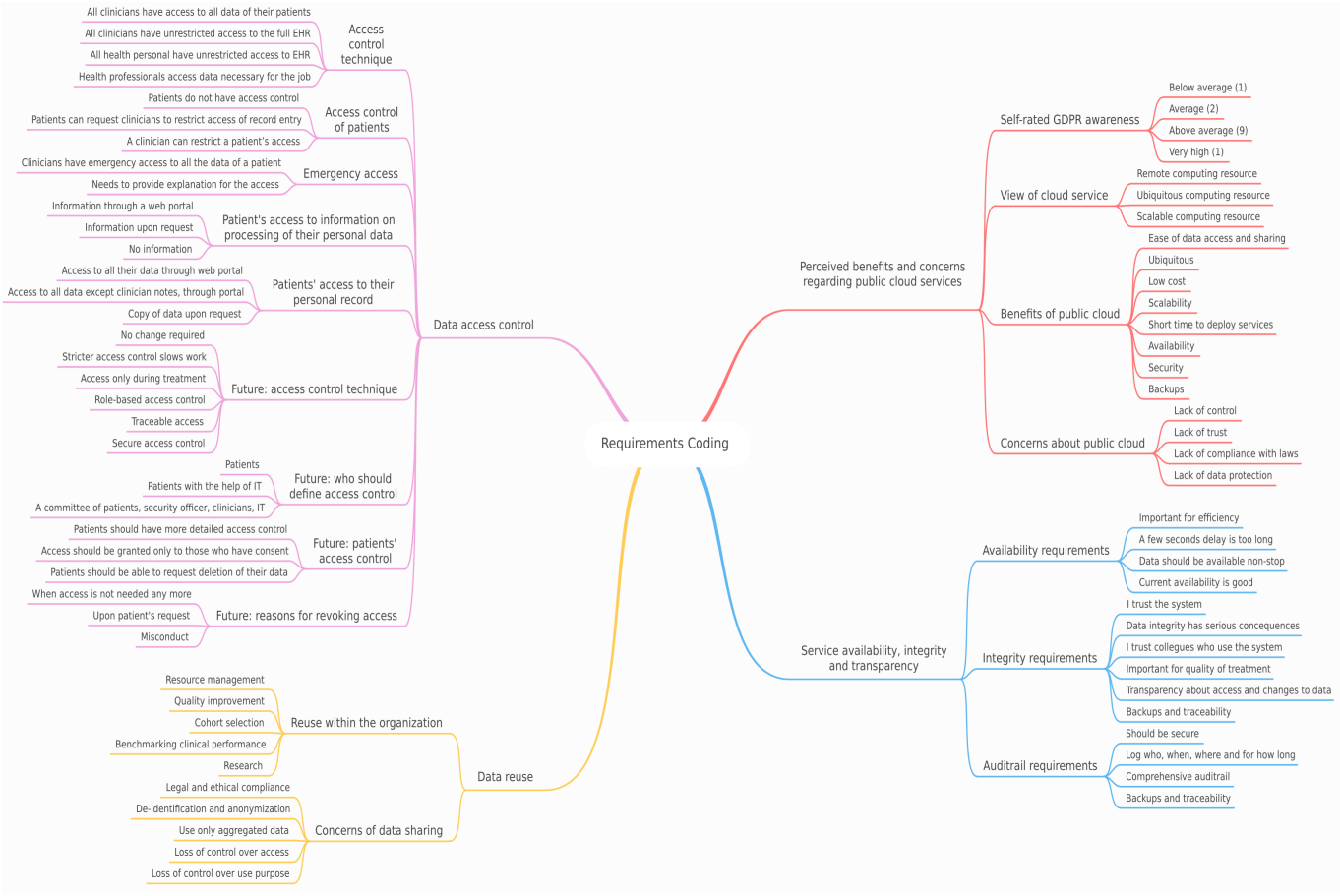

Fig. 1. Four themes and codes extracted from the interviews

concern that more strict access control could slow down their work. A compromise could be to restrict access to the treating team and revoke access once treatment is complete.

> *"I'm very concerned if it would be stricter access control. It's not very easy to see an overview of all documents I need. Stricter access control will take me longer to do my work."*
>
> *"When the patient is no longer under treatment, and there is no need for the data, then access should be revoked."*

According to the interviews, in some cases, patients could get access to information on the processing of their personal data. This could be done through an online portal, or patients could submit a request for it. In other institutions, patients were not able to access such information. However, in terms of access to the actual patient record, this could be done either in the portal or by request, but the clinician notes would not be available to the patient.

One interesting idea emerging from the interviews is the involvement of patients in defining access control. It was suggested that in the future, patients should determine access control to their EHR by themselves or with the help of a system administrator, security officer or clinicians. In addition, patients should be able to request their data to be deleted or to revoke access. The main reasons cited for revoking access were for those who did not need access anymore, due to the patient's request, or in cases of misconduct.

> *"If the user is abusing his access to the data – intentionally or unintentionally – or negligently opening access to the data, even if it doesn't get leaked; the potential negligence should be a course for revoking access."*

D. Service availability, integrity and transparency

Participants pointed out that data always has to be available, and that current availability was good. Emphasis was also made on how fast the service should be, for example, a 2.5-seconds wait would be considered long under high pressure, and a 15-seconds delay would be totally unacceptable.

> *"The information should be there instantly. If you have to wait two and a half seconds to get the data, it is ohhh ... it is very long."*

An underlying issue discussed was that clinicians and other health professionals must be able to trust the integrity of the system. System integrity has severe consequences for the quality of treatment; therefore, backups and traceability are important. Since colleagues rely on each other, the identity of colleagues who update or delete the data should be transparent. However, some participants did not know how to access the audit trail and logs.

> *"It should be possible to see who accessed the data and made changes and also who deleted something."*
>
> *"I trust my colleagues. Theoretically, it can be very serious if there is no integrity."*

E. Data reuse

Several data reuse purposes were reported, including for resource management, quality improvement, benchmarking clinical performance, recruiting study participants and general research. However, several concerns also arose from the discussion. The number-one issue was compliance with the legal and ethical requirements, for example, the difficulty to control access and purpose of data use once the data is disclosed. De-identification and anonymization were identified as important for data reuse. Further, some pointed out that only data in aggregated form should be used for secondary purposes. Aggregated use is hardly possible for medical image and medical signal data, however.

> *"...lose track of who has the data, because now there is no way to revoke access. Once the researcher has received the data, the hospital trusts that the researcher will not use the data for any other purpose."*
>
> *"The major concern is to lose track of the data and expose a patient."*

F. Comparison with GDPR and ISO 18308:2011

For the three identified GDPR aspects (rights of the data subject, controller and processor, and transfer of personal data to third countries or international organizations), the participants' perspectives were generally in harmony with the regulation. Most of the themes were related to "rights of the data subject" since the clinical work is closer to the patient. We found the same consistency with the ISO 18308:2011 standard.

G. Differences between countries and institution types

There were no notable differences in perspectives among the three countries. However, there was a difference between large institutions and smaller GP offices. We noted that in smaller GP offices, clinicians tended to have more control of the EHR system compared to clinicians at larger hospital or national EHR systems. Health professional in the offices had almost unrestricted access to the EHR records of all patients. In addition, access control is mostly driven by the clinician, even though patients can ask access to be restricted. For example, a patient may ask restricted access for a health professional who is also a neighbour.

IV. Discussion

Results showed that the participants were generally knowledgeable about new computing platforms like cloud computing, and conscious about the new regulations like the GDPR. According to the diffusion of innovation theory [9], which focuses on complex innovations in health services, the users must see a relative advantage in the new system compared to the old system. Our results aligned with this theoretical expectation and showed that participants were well aware of the limitations of current systems and the promise of e-health cloud services. It should be noted that the participants were experts in neither computer security nor law, but most rated themselves as having above-average awareness of the GDPR. In the succeeding subsections, we describe how the user perspectives relate to keys aspects of the GDPR and ISO 18308:2011.

A. Rights of the data subject (GDPR)

Some of the themes and requirements that emerged from this study corroborate findings in recent studies. For instance, a recent study by Desai et al. [10] showed that from the perspective of health professionals, accessing health data from multiple locations and on multiple devices is a desirable benefit of cloud computing. However, our findings diverge from theirs when it comes to EHR access control. Whereas Desai (ibid) found that healthcare professionals preferred permissions to be caregiver-controlled, our study showed that healthcare professionals preferred access control to remain vested in the patient. In cases where the patient lacks competence, an IT administrator or health professionals could assist. This is an important difference because one study places power in the caregiver's hands while the other gives power to the data subject; the patient. A possible explanation for this divergence may stem from the different stances on patient empowerment in the countries where the studies were conducted, i.e., the US versus Europe.

In terms of patient access to data, the GDPR (Art. 15) requires data subjects to have access to information about themselves. This was enabled through web portals for some institutions. While at the other institutions patients were not able to readily access their data, they could request such access. Patients could ask their data to be deleted from the health institution, and this complies with (Art. 17). However, it was not clear if the patients were able to have a data export in a structured, machine-readable manner, for the health institutions to comply with (Art. 17) – the right to data portability. It is conceivable that patients could export their data in a structured format because of institutional web portals made for patients. In addition, patients could ask for their data to be restricted, and this complies with (Art. 18). When data is restricted, no more processing is allowed, but the data may be kept in storage.

B. Controller and processor (GDPR)

In GDPR terms, the healthcare institution is a "data controller", and the cloud service provider is a "data processor". From our interviews, it appeared that participants were generally fearful that the data processor might have more control over the data than the data controllers, and further, that the processor would be able to view sensitive health data, and use it for commercial purposes or some other gain.

The GDPR offers protection for these kinds of foreseeable threats. For instance, (Art. 25, Art. 32) require the controller to exercise due care to protect data using state-of-the-art methods. Health data could be encrypted or pseudonymized before being uploaded to the cloud provider's platforms. Participants discussed using data aggregation and de-identification when it comes to secondary use of health data. According to GDPR (Art. 29), the processor may not process personal data except when instructed by the controller.

Another fear that came out from the interviews was that the processor might not have the capacity to fulfil all ethical and legal requirements for handling health data. Today, contracts must be signed between the controller and the processor to ensure all legal requirements are satisfied. In addition, the processor could have specific relevant certifications and monitoring mechanisms to demonstrate that they are compliant (see Art.42).

In addition to concerns regarding a cloud service, participants were also worried about access to patient data by healthcare professionals, but outside of the context of treatment. This is a well-recognized problem, and a recent study by Correia et al. [11] examined undue access to patient data using audit trails as the basis. While participants pointed out that any abuse of data should result in access revocation, the GDPR (Art. 333 and Art. 34) goes further and mandates that any such misuse or breach be reported to authority and the affected data subjects be notified "without undue delay".

C. Transfer of personal data to third countries or international organizations (GDPR)

Transferring personal data outside of the healthcare institution can pose challenges. The very nature of cloud computing makes data location transparent to the user, that is, the user does not see how data components are composed. Often the data is distributed over several geographical locations, and this may cause compliance complications. Generally, GDPR does not forbid the transfer of data to cloud systems domiciled outside Europe. However, for all lawful processing outside the EU, consideration is given to the stability and capacity of the countries to protect the data.

D. EHR business objectives (ISO 18308:2011)

Among healthcare system objectives, the ISO standard requires authorized users to have access appropriate to the context. Our interview results showed the clinicians also meant access to the EHR should be treatment-based, and for the duration of the treatment only. This can also be viewed in the prism of shared care where all authorized persons in the care teams must have complete information to do their job.

Another aspect in the ISO standard is how healthcare systems should aim to support thorough auditing and secondary use of data. There was consensus among the participants on the importance of secondary use of data for scientific research and improving quality of care. ISO further calls for professional learning based on specific patient cases. This can present challenges since access to data is based on direct treatment or care. The records or cases should be de-identified to access cases from the EHR. However, de-identification of clinical data, especially free-text clinical notes, is still an open research problem [12].

The ISO standard also provides guidelines for citizen inclusion, where patients should be able to view their data and participate in their own care. This objective is consistent with the goals of the GDPR as well as the perceptions of the participants. Also, the ISO standard calls for the patient to be responsible for specifying access control rules. This is something with which our participants also agreed, but it was not clear if it was common practice to have patients define access control rules.

E. Requirements for an EHR architecture (ISO 18308:2011)

An important aspect to highlight regarding the guidelines for an EHR architecture is the support for audit trails. Audit trails must be detailed showing when and where the record was created or updated, and by whom. Participants supported detailed audit trails that showed work done by their colleagues with whom they shared care for a patient. Since records can be updated from multiple locations when using cloud infrastructure, clinicians would like a better understanding of the context of care.

Although participants and the ISO standard agree on patient data management based on consent, the ISO standard goes further to ask for the representation of consent for creating a health record, and mechanisms for tracking that consent. In contrast, the GDPR permits processing data even without consent if there are other legal grounds permitting such processing. For practical reasons, consent can be implied and implemented in access control policies. However, it was not clear if all the EHR systems the participants worked with had any explicit or implicit consent that could be readily inspected.

F. Differences between countries and institution types

The access control differences we noted between large and small institutions can be explained by the organization of the healthcare systems. A GP is responsible for a set of patients, and, therefore, have full access to their data at any time. When the GP is not available, his colleagues in the office may have to treat his patients, therefore, have access to data of patient who are not on their list. In contrast, patients get treated at hospitals for an episode of care. Therefore, access to patient data is provided for the duration of the episode. Application of security requirements should consider the risks

versus clinicians' work efficiency since GPs are the "first line of defence" for patient care in the participating countries.

G. Secure and privacy-preserving framework for e-health cloud

The ASCLEPIOS project [8] is developing a cloud-based e-health framework based on the requirements collected from the user perspective and the requirements of the GDPR and ISO standard. The framework uses symmetric searchable encryption (SSE) scheme for encrypting health data before storage on cloud, which allows searching on encrypted data while protecting privacy [13]. The framework ensures the security of an encryption key using attribute based encryption (ABE) before storage on a trusted execution environment of a CSP. The ciphertext of the encryption key contains policies that describe who (defined by a set of user attributes) can decrypt the ciphertext. Therefore, only a user who has a private ABE key containing attributes that satisfy policies included in a ciphertext can decrypt the cipher text and, consequently, use the SSE key for decrypting the health data encrypted with the SSE key. The framework in addition protects access to encrypted SSE keys and to the ciphertext of encrypted EHRs, using an attribute-based access control (ABAC) engine that decides who, from where and when can request encrypted health records and the ciphertexts of their SSE keys [14], [15]. This constitutes a context-aware authorization step before granting access to sensitive data. The framework also uses functional encryption (FE) [16] to compute population level statistics on encrypted health data of a single healthcare institution stored on cloud while protecting privacy. The framework combines secure multi-party computation [17]–[19] and FE to support privacy-preserving distributed statistical computation on health data of multiple healthcare institutions stored on cloud.

V. Conclusion

While no real differences in perceptions were noted among the participating countries, the noted access control differences between large institutions and small institutions have implications for compliance with regulations and best practice. Current unfettered access to the EHR at small institutions is not optimal and warrants further inquiry.

Healthcare professionals with no specialist computer security or legal backgrounds demonstrated a good grasp of cloud computing and regulations from GDPR and guidelines from ISO 18308:2011. While their perspectives were in harmony with GDPR and the ISO standard, the participants' above-average familiarity with GDPR may have skewed our results. Further investigation with a representative sample of clinicians is required to inform any targeted information and educational campaigns.

This study provides unique insights from the user perspective, which could be collated with requirements from the GDPR and the ISO standard, to form a user-centred framework for a secure e-health cloud service.

Acknowledgment

We would like to thank the data subjects for their willingness to participate in the interviews. We also thank members of the ASCLEPIOS project.

References

[1] P. Mell and T. Grance, "The NIST definition of cloud computin". 2011.
[2] F. Sadoughi and L. Erfannia, "Health Information System in a Cloud Computing Context." Stud Health Technol Inform, 2017. 236: p. 290-297.
[3] L. Griebel, et al., "A scoping review of cloud computing in healthcare." BMC Med Inform Decis Mak, 2015. 15: p. 17.
[4] Y. Al-Issa, M.A. Ottom, and A. Tamrawi, "eHealth Cloud Security Challenges: A Survey." J Healthc Eng, 2019. 2019: p. 7516035.
[5] E.J. Schweitzer, "Reconciliation of the cloud computing model with US federal electronic health record regulations." J Am Med Inform Assoc, 2012. 19(2): p. 161-5.
[6] M.H. Kuo, A. Kushniruk, and E. Borycki, "Can cloud computing benefit health services? - a SWOT analysis." Stud Health Technol Inform, 2011. 169: p. 379-83.
[7] E. AbuKhousa, N. Mohamed, and J. Al-Jaroodi, "e-Health cloud: opportunities and challenges." Future internet, 2012. 4(3): p. 621-645.
[8] "ASCLEPIOS." https://www.asclepios-project.eu/ (accessed Sep. 18, 2020).
[9] T. Greenhalgh, et al., "Introduction of shared electronic records: multi-site case study using diffusion of innovation theory." BMJ, 2008. 337: p. a1786.
[10] A.D. Desai, et al., "Caregiver and Health Care Provider Perspectives on Cloud-Based Shared Care Plans for Children With Medical Complexity." Hosp Pediatr, 2018. 8(7): p. 394-403.
[11] L.S. Correia, R.C. Correia, and P.P. Rodrigues, "Illegitimate HIS access by healthcare professionals: scenarios, use cases and audit trail-based detection model." Procedia Computer Science, 2019. 164: p. 629-636.
[12] F. Dernoncourt, J. Y. Lee, O. Uzuner, and P. Szolovits, "De-identification of patient notes with recurrent neural networks," J. Am. Med. Inform. Assoc. pp. 596–606, May 2017.
[13] A. Michalas, "The lord of the shares: combining attribute-based encryption and searchable encryption for flexible data sharing," in Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, 2019, pp. 146–155.
[14] Y. Verginadis, I. Patiniotakis, P. Gouvas, S. Mantzouratos, S. Veloudis, and et al., "Context-aware Policy Enforcement for PaaS-enabled Access Control." IEEE Transactions on Cloud Computing, 2019, pp. 1-16.
[15] E. Psarra, Y. Verginadis, I. Patiniotakis, D. Apostolou, and G. Mentzas, "A Context-Aware Security Model for a Combination of Attribute-Based Access Control and Attribute-Based Encryption in the Healthcare Domain," in Web, Artificial Intelligence and Network Applications, 2020, pp. 1133–1142.
[16] D. Boneh, A. Sahai, and B. Waters, "Functional Encryption: Definitions and Challenges," Theory of Cryptography, vol. 6597, 2011, pp. 253–273.
[17] M.A. Hailemichael, K.Y. Yigzaw, and J.G. Bellika, "Emnet: a tool for privacy-preserving statistical computing on distributed health data." Proceedings from The 13th Scandinavian Conference on Health Informatics, 2015, pp. 33–40.
[18] K. Y. Yigzaw, J. G. Bellika, A. Andersen, G. Hartvigsen, and C. Fernandez-Llatas, "Towards Privacy-preserving Computing on Distributed Electronic Health Record Data," in Proceedings of the 2013 Middleware Doctoral Symposium, 2013.
[19] K. Y. Yigzaw, A. Budrionis, L. Marco-Ruiz, T. D. Henriksen, P. A. Halvorsen, and J. G. Bellika, "Privacy-preserving architecture for providing feedback to clinicians on their clinical performance," BMC Medical Informatics and Decision Making, 2020.

APPENDIX 1: QUESTIONNAIRE USED AS INTERVIEW GUIDE

Organizational characteristics:

1. Please describe your organization?
2. How many employees work in your organization?
3. How many IT staff does your organization have?
4. Please describe your job title.
5. Please briefly describe your responsibilities in organization.

Awareness of data protection regulations:

6. Are you aware of the relevant laws and regulations for health data processing, such as general data protection regulation (GDPR)? If yes, how do you rate your level of knowledge about the contents of the regulations?

Cloud service:

7. Please tell me your view of what a cloud service is. Trigger words: ubiquitous, on-demand, scalable, accessibility, computing resource, software as a service, platform as a service, infrastructure as a service, private cloud, public cloud, hybrid cloud.
8. Does your organization have e-health systems, such as electronic medical record (EMR) system, and/or health data hosted in the cloud? If the organization does not use a cloud service: a. Does your organization plan to migrate an e-health system or health data to a cloud service?
If the organization has no plan for using a cloud service in the future, do you know why not?
If the organization uses or plan to use a cloud service, do you know why?
9. What do you consider to be the benefits of migrating e-health systems to the cloud? Possible answers (do not reveal to data subjects): reduced IT costs and staff, better information security, robust disaster recovery, access to scalable computing resources, short time to deploy services, regulatory compliance, ubiquitous access, etc.
10. Do you have security and privacy concerns when storing patient data in the cloud? If yes, what are your major concerns? Possible answers (do not reveal to data subjects): lack of control on data processing, compliance with regulations, trust on cloud service providers, etc.

Confidentiality:*Personal data must be secured against unauthorized processing.*

Access control:

11. What access control techniques does your organization's current EMR system support? Comment: the question aims to know the techniques/procedures regulate who can view what data (a certain part of data).
a. What kind of access control do patients have on their data? Comment: the question aims to know whether patients can decide who views what data (in the current EMR system).
b. Please tell me about emergency access to patient data. Comment: during emergency situations, a clinician who does not have access right may get access to patient data. The question aims to know whether clinicians have emergency access (in the current EMR system).
c. Do patients have access to information such as who accessed their data and reasons for access? Comment: The question aims to know whether patients get access logs of who has accessed their data and why (in the current EMR system). Data access reasons include clinical care, research, and quality improvement studies.
12. What kind of access control do you think is necessary for future systems?
a. Who should define access control? Comments: possible answers include clinicians, patients, and system administrators
b. What level of access control should patients have on their data? Comment: the question aims to know how detailed access control should a new system gives to patients.
c. How detailed access control is necessary? Comment: This question aims to know the level of detail of the access control a new system should have. For example, should the access control be at a department, clinical speciality (e.g., nurses, doctors) or individual level.
d. When should access grant to an authorized user be revoked? Comment: this is aimed to understand when is access granted to a person and his/her access revoked. For example, should access be granted when a patient has an appointment? And should the access be revoked immediately after the appointment?

Data processing:

13. Does your organization see value in generating statistics from patient data?
a. Can you explain the purposes of such statistics?
14. What do you think about patient data sharing for secondary uses?
a. What are your security and privacy concerns of data sharing?

Accessibility (availability): *personal data must be available to authorized personnel who require it for their work.*

15. What are your availability requirements or expectations for health data?

Integrity: *Personal data must be secured against accidental and unlawful destruction, loss, or alteration;*
Traceability: *documentation of changes to data*

16. What do you require to be confident about the integrity of health data?
17. What do you think about the use of access logs for data integrity and traceability?

Definitions

GDPR 4(2) states that 'processing' means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
The NIST definition of cloud computing - https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf