Cloud Computing Framework for e-Health Security Requirements & Security Policy Rules Case Study: A European Cloud-based Health System

Dimitra Georgiou and Costas Lambrinoudakis

July 26, 2020

Cloud Computing Framework for e-Health Security Requirements & Security Policy Rules Case Study: A European Cloud-based Health System

Dimitra Georgiou[1] [0000-1111-2222-3333] and Costas Lambrinoudakis[2][1111-2222-3333-4444]

Systems Security Laboratory, Department of Digital Systems
School of Information & Communication Technologies
University of Piraeus, Piraeus, Greece
[1]dimitrageorgiou@ssl-unipi.gr, [2]clam@unipi.gr

Abstract. The final few years, Information and Communication Technology (ICT) have delivered the concept of central enterprise model in e-health. Health-care is increasingly being supported via IT functions and new technologies, such as Cloud Computing. But sharing sensitive private data in Cloud Computing can be risky, when an unauthorized person gets access to this information and uses this in a different way than those supposed by the Providers. Numerous nations are sharp to go their typical health care services to the modern innovation of Cloud Computing, in order to move forward the first-class of care and to limit the cost. In any case, these possibilities introduce new safety risks and require a special treatment of safety issues, which cannot be ignored. Our work focuses on analyzing the challenges when using Cloud Computing in e-health systems and on moderation of these risks. In this paper, we present a list of the main security requirements that have to be viewed when migrating an e-health system to a SaaS Cloud Computing environment by means of each Health-care Providers and Cloud Service Providers and at the same time we propose some basic provisions to mitigate the significant risks.

Keywords: Cloud Computing, e-Health, Security, Requirements, Policy Rules.

1 Introduction - Information Privacy in Health Informatics

The healthcare environment is undergoing fundamental changes. The previous years, doctors and hospitals used to have many papers and envelopes to keep the health of their patients and every time that a patient used to change doctors, there were nothing about their history of their health. Nowadays, many countries in order to improve their services on e-health, incorporate new technologies into their traditional medicine care. Internet technologies try to protect patients' privacy and confidentiality of medical data, while at the same time improve the quality of care. The benefits provided by the Internet, however, come with a significantly greater element of risk to the integrity of information. Thus, information security and privacy remain a high concern for citizens regarding their health data [1][2]. Unfortunately, traditional security mechanisms are not appropriate to meet patients' requirements in new technological advances in e-Health Care services, so the creation of a general e-Health Cloud Security Policy that defines the security requirements for Cloud Computing e-health system is needed. To better understand the developments in terms of e-Health, it is necessary to understand what e-Health is and what exactly e-Health Security Policy is in the area of these new technologies. When we mention the term e-Health, we mean the use of information technologies across health related functions and activities [3].

An electronic Health service system, is a collection of components working together to implement the e-Health services. As data is processed into practical information by the system, authentication and authorization become the essential concerns of the e-Health service systems [4]. In addition, the European Commission defines e-Health very generally as "*The use of modern information and communication technologies that meet needs of citizens, patients, health care professionals, health care Providers, as well as Policy makers*" [5].

To use properly and effectively an e-health system, we need an appropriate Health Policy. A Health Policy has been defined as '*a set of statements, directives, regulations, laws, and judicial interpretations that direct and manage the life cycle of e-health*' [6]. In the area of health, the creation of an e-Health Policy that balances the need for access (authorization) with the needs and the rights of the citizens, is the biggest challenge. There are several examples of countries that have national e-Health strategies some of these are Italy, France, UK, while other has introduced the electronic health card, like Germany [7].

New technologies, such as Cloud Computing, could improve e-Health services to their patients. Health data will be more easily accessible by doctors thus supporting a better diagnosis and treatment for their patients. Cloud-based e-Health services could change the traditional Health environment and could bring a lot of advantages [8][9][10]. The industry may considerably improve the access to information and patients will have improved diagnosis, treatment and faster decision making responses from assigned medical professionals. However, despite the potentially high value of the new technological development of Cloud Computing, in the area of e-Health, the security of medical information, as well as data handling, is a serious issue [11][12][13][14]. In order to achieve the security levels in the medical environment, it is necessary to identify carefully the security requirements for this.

In our research, we study the protection of the confidentiality of patients' information and we facilitate the processes of the e-Health Cloud system with some suggestions for Health Cloud Providers. We analyze the security requirements of a Cloud-based System, from the perspective of the Service Provider, using as an example, the case study of an e-Health Cloud system in Europe. In particular, in this paper based on the list of threats published by our previous papers [15][16][17], we discuss how each category of threats can be linked to specific security requirements. Lastly we provide a set of security policy rules for the presented security requirements, that we consider significant for any growth methodology that supports the design of secure and private Cloud. Although, the list of the presented requirements is not the final, we believe that this list provides a good basis for any

Developer that would like to consider inclusion of Cloud security and privacy analysis in their methodology.

Section 2 provides a brief overview of the background of Information Systems in Europe. Section 3 presents the Cloud Computing implementation issues with basic Cloud computing characteristics. Section 4 discusses the major categories of threats according to our Methodology and provides a clear linkage with a set of Security Requirements. Section 5 presents specific security policy rules related to the set of security requirements for every category of threats. Finally, Section 6 presents areas for future work and concludes the paper.

2 Case Study of Europe: e-Health Cloud-based System

2.1 Background of the Information Systems in Europe

In Europe, the European Union (EU) has endeavored to promote the implementation of e-Health within the 27 Member States by making e-Health a key part of EU Health Policy [18][19][20][21]. The big challenge and the vision of the EU is to achieve the wide spread adoption of e-Health systems across Europe as part of the EU's Flagship initiative 'Digital Agenda for Europe'[22][23][24]. Also a key ambition of the EU Policy is the provision of better care services at the same or lower cost [25]. The 2004 EU e-Health Action Plan was the first initiative that set in motion the EU's plans to encourage European co-operation on Health Care issues [26]. In our research, we illustrate as an example application scenario, the European Union e-Health system and the implementation strategies that use across the EU and European Economic Area Member States.

So, in this paper, we will present an existing e- Health Information System, the system in Europe, that consists of 27 national e-Health programs, as the number of European Countries and illustrates the overall framework. Then, we will present how this Information System would be with the use of Cloud Computing, what the new Critical Security Requirements associated with the aforementioned threats are and what the proposed solutions for these Cloud Computing security requirements are. In this scenario, the approach of a European system conceptualizes the health-care system as a value system of a variety of Health Service Providers, each of which has to manage its own health system. As depicted in this research, this health system, which consists of individual health Service Providers, promotes good health and long-term care services, supports disease prevention and provides healthcare. The European Commission's e-Health Action Plan mentions the lack of awareness and confidence in new technologies among professionals and citizens as a barrier to adopt them [27].

The previous years, the European Commission (EC) has established working parties and expressed its intention for information development in all public health programmes [28][29][30]. Examples of the term of e-Health according to the European Commission's e-Health Taskforce are: clinical information systems, e-institutions, Telemedicine and Homecare systems, Integrated regional/national health information networks (Fig.1), Secondary usage non-clinical systems [31]. Other examples also include: electronic health records, portable communicable systems including those for medical implants, health portals, and many other ICT-based tools assisting disease prevention, diagnosis, treatment, health monitoring and lifestyle management. This system makes it difficult to share information beyond organizational boundaries.

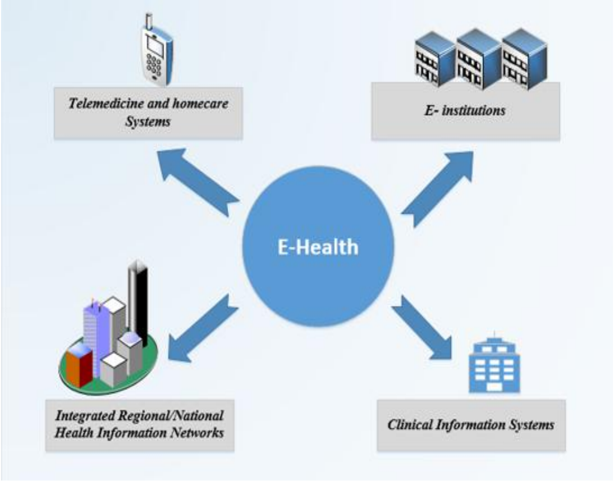
Telemedicine and homecare Systems
E- institutions
E-Health
Integrated Regional/National Health Information Networks
Clinical Information Systems

Fig. 1. E - Health example types

The increasing prevalence of ICTs can have transformative impacts on many industries, including health-care where ICTs can deliver citizen centrist health-care and foster a dyadic information symmetric physician-patient relationship [32].

3 E-Health Cloud Computing Implementations Issues

Cloud Computing has been widely recognized as the next generation's technology and it offers several advantages to its users. Cloud Computing can also offer many chances to expand health care services, due to its characteristics that are particularly appealing to the needs of Health-care Providers. On a Cloud-based-health system, the user does not manage or control the Cloud infrastructure, but mainly the software services are provided by the Provider to its end users, clinicians and patients [33] [34] [35] [36] [37] [38] [39].

In addition, Cloud Computing is characterized by consumers who use Cloud services as needed, who consume shared resources as a service and pay only for what they used and who access services over a networked infrastructure. Cloud adoption also provides the ability to exchange data between different and distinct systems. In health-care, it can be implemented as a way for maintaining or managing patient information, at different locations. In Fig. 2 we present a Cloud-based Health Information System that communicates with the following actors (doctors, patients, medical personnel) and hospitals via a lot of Clouds and via network connections. To provide consistent and coordinated care at a reasonable cost, Providers must be able to share patient's medical information freely while maintaining information security of their data.

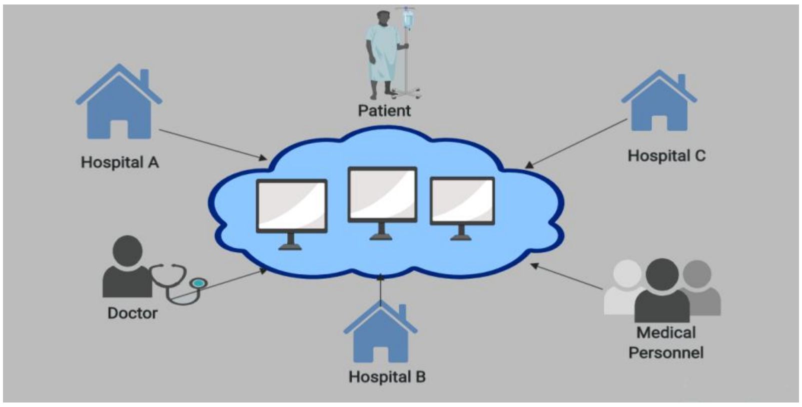

Fig. 2. A Cloud -Based Health System

The proposed e-Health Cloud-based system presents the end users (authorized Doctors, Medical Personnel and patients) that could take part in SaaS Cloud-based Health System. All the stakeholders are been navigated through the sharing hospitals and the whole Information systems. As we can understand, the most important component to this system is to ensure the security and to guarantee the confidentiality of the data, due to the fact that we have to deal with sensitive data and the protection of stored information comes as a top priority. And how can we succeed this? By defining, the assets that we want to protect, the possible security requirements of such a system and the corresponding Security Policy Rules. The assets of such Information system, based on Cloud Computing, is described to ensure the availability, integrity, authentication, confidentiality of the service and the e-transformation of records. The security requirements and the proposed solutions for such a system will be analyzed in the next parts.

4 Major Security Requirements in Cloud-based Health Systems

Whatever the choices of the organization or hospital are, there are some security challenges that need to be addressed, when somebody decides to implement a Cloud-based health system. This study aims to support the development of an EU Cloud-based Healthcare System by identifying the necessary key requirements relevant to build up a comprehensive system that supports health policy making.

At the proposed Methodology of our Security Policy, we presented all the Cloud security threats according to the list of threats published by Cloud Security Alliance [40], Gartner [41] other relevant literature and some new Cloud-specific security threats based on our research. Then we categorized threats in 4 Categories (Figure 3) according to our Policy Methodology and finally we linked these Categories with the requirements related to critical areas.

This report contributes to the definition of a requirement Landscape, by providing an overview of current and emerging security requirements applicable to Cloud-based technologies. The goal of this report is to deepen our understanding into the security requirements that affect Cloud-based Health systems and to provide good practices and recommendations for those requirements that are considered important or emerging. In our research, we have decided to define a list of 19 different threats and only some of them are specific to Cloud Computing, while the rest can also be found in traditional distributed systems.

In addition, to support the challenges of Cloud-based Health Systems, we have defined a set of security requirements (specific for every category of threats), that an analysis and design methodology should support. It is worth mentioning that we only focus on a list of requirements related to modeling and analysis of security and privacy-related concern. In Fig.3, we present the four Categories-Gates of threats that proposed in our General Security Policy Methodology and then at the next part we describe the security requirements involved in them.

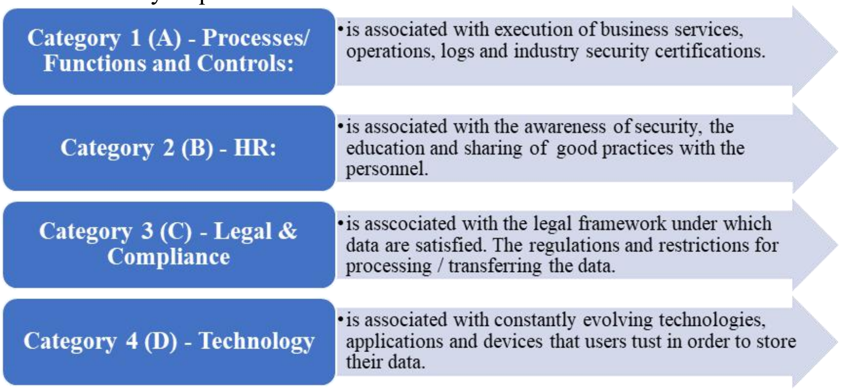
Category 1 (A) - Processes/ Functions and Controls:
•is associated with execution of business services, operations, logs and industry security certifications.
Category 2 (B) - HR:
•is associated with the awareness of security, the education and sharing of good practices with the personnel.
Category 3 (C) - Legal & Compliance
•is asscociated with the legal framework under which data are satisfied. The regulations and restrictions for processing / transferring the data.
Category 4 (D) - Technology
•is associated with constantly evolving technologies, applications and devices that users tust in order to store their data.

Fig. 3. Four Categories of threats according to our Security Policy Methodology

Understanding and documented the security requirements of an e-health Cloud System, gives a solution targeting to each threat and at the same time maps them with the provisions of the Cloud Security Policy. In each category of threats is necessary to ensure what security requirements are covered by the Cloud Provider according the following security measures. In the following analysis, while there are many security concerns in the cloud, this report focuses only on four specific related threats that are representative of every category of threats, according to our Security Policy Methodology. We selected the following threats, as representative threats of a Cloud-based Health System, because they are crucial for a Cloud Computing system and they have the maximum likelihood to occur:

Threat #1: The Abuse of Cloud Services - **Category 1 (A)**
Threat #2: Insufficient Knowledge - **Category 2 (B)**
Threat #3: Data Loss - **Category 3 (C)**

Threat #4: Back up Vulnerabilities - **Category 4 (D)**

In the Analysis that follows, we present the security requirements involved in a Cloud-based Health system (Fig.4). Although that, there are different security tasks for every Service Model of Cloud Computing (IaaS, PaaS, IaaS), in our research we only focus to tasks that a Cloud Provider should implement for a SaaS Service Model.

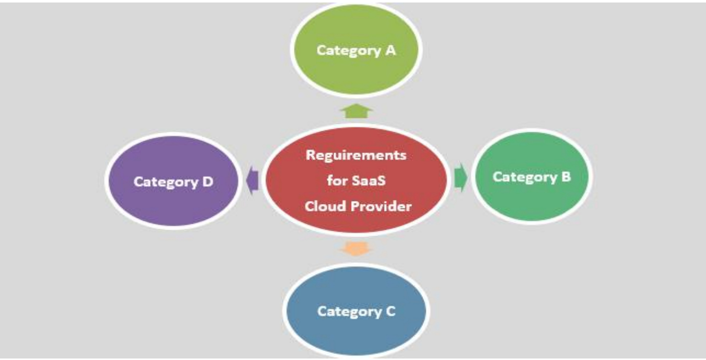

Fig. 4. Requirements for every Category of Threats

Clouds face a multitude of requirements in Cloud-based systems. We have identified the following requirements associated with the aforementioned threats of **Category A (Processes /Functions & Controls) for Cloud-based health systems:**

- **A1. Data controls:** when health data are stored on Cloud, appropriate controls need to be in place. Data are at the core of security concerns for any e-health system, whatever form of infrastructure is used. The distributed nature of the cloud computing and the shared responsibilities that involves, bring the security considerations both to data at rest and also to data in motion, on the priority.
- **A2. Disaster recovery procedures:** Having Disaster recovery procedures in Cloud-based health system, reduces the need for data center space, IT infrastructure and IT resources, which leads to significant cost reductions, enabling smaller hospitals to deploy disaster recovery options.
- **A3. Unauthorized access by e-health professionals:** Cloud Providers are responsible for separating their clients in multitenant situation. Health data are of a sensitive nature, so a Cloud Provider may not allow direct access to information to everyone, without appropriate authorization.
- **A4. Ubiquitous network connectivity to the hospital:** consumers evaluate the external/internal network controls of a Cloud Provider. In a Cloud-based Health system, each user's requirements will be different, but it is recommended that users evaluate the internal network controls of a Service Provider such as: to protect clients from one another, to protect Provider’s network, to monitor for intrusion.
- **A5. Quality of service and reliability:** one of the challenges posed by a Cloud-based health system is QoS, which is the problem of allocating resources to the application to guarantee a service level such as performance, availability, reliability.

- **A6. Data Centers - unauthorized entities:** According to the explanation of Cloud Computing by NIST [38], *resources refer to computing applications, network resources, platforms, software services, virtual servers and computing infrastructure*. It is a virtualization of resources, which the end user has on-demand access. In the e-Health Cloud System, the unlawful entities may obtain unauthorized access to the patients' data.
- **A7. Digital signatures/ certificates:** A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI). Health-care professionals can gain access to health data using a digital certificate.
- **A8. Malicious insider (doctor, staff, family member):** A malicious insider is well known to most organizations, He could access the sensitive data, steal information, sell the data to other parties or perform number of malicious activities.
- **A9. Abuse of Cloud Services**: Cloud Computing Providers are actively being targeted, because their relatively weak registration systems facilitate anonymity and Providers' fraud detection capabilities are being limited.
- **A10. Lack of user control:** Ownership and accountability are not well defined or applied even in traditional IT systems. Thus, Providers should examine what they are trying to control in the system: over data, over functionality, over assets.

The Critical Requirements associated with the aforementioned threats of Category B (HR) for Cloud-based health system are the following:

- **B1. Lack of trust by health care professionals:** has proven to be one of the substantial barriers limiting the extensive adoption of Cloud Computing. With regard to the Cloud Provider trustworthiness means primarily considering security and privacy aspects when offering cloud services.
- **B2. Lack of awareness:** is a key barrier to Cloud usage. Medical staff and doctors are confused by the term Cloud Computing, which is preventing them from taking the necessary steps to implement the technology.
- **B3. Lack of Segregation of duties:** In the Health environment the staff believes that there is no need in segregation of duties in the technological environment
- **B4. Lack of Education in Information System and alertness:** Health professionals should be educated in the use of Information systems and their risks in order to be alert and respond to security incidents,
- **B5. Lack of Organizational Structure & Responsibilities:** Organizational structure creates the company hierarchy for authority and responsibility.
- **B6. Lack of Confidentiality agreement prior to being given information:** When drafted and used properly, confidentiality agreements are an effective way to protect confidential information. Parties should outline their respective obligations.
- **B7. Code of contact of proper use:** defines how a company's employees should act on a day-to-day basis. It is unique to the organization it represents

The Critical Requirements associated with the aforementioned threats of Category (Legal Requirements & Compliance) for Cloud-based health system are the following:

- **C1. Loss of governance:** The cloud consumers need to be sufficiently in control of the IT systems.
- **C2. Data jurisdiction issues:** are mostly related to location of data and the specific laws that apply in that location.
- **C3. Intellectual property rights:** Cloud-stored data often transferred from country to country, some with weak Intellectual Properties laws or enforcement.
- **C4. Compliance with security policies: S**ecurity policy provides Health organizations with a framework to operate its business and protect patients without interruption from bad incidents.
- **C5. Data protection:** used to protect stored, static and moving data. It is designed to implement data storage, protection and security methodologies**.**
- **C6. Data loss:** is any process or event that results in data being corrupted, deleted or made unreadable by a user, software or application. However, there are ways to minimize the risk of data loss and ensure the security of data in Cloud storage.
- **C7. Data Breach/ data separation:** Cloud computing gives organizations the ability to run workloads and manage data anywhere without significant computing.
- **C8.Third party controls:** Using these controls can help to identify procedural errors which, if undetected could lead to the reporting of incorrect patient results.
- **C9. Lack of industry standards and certifications:** Without any industry cloud standards, vendors have the possibility to build cloud services on software stacks that are not compatible with the one used in public Clouds.
- **C10. International Regulations:** There are federal, international laws that impose responsibilities to both cloud computing tenants users and providers. Especially those related to the data you collect, store and process.
- **C11. Complexity to ensure compliance:** Decentralization, scaling and other characteristics in Cloud add further complexity to ensure the compliance.
- **C12. Control data:** means implementing policies of governance to ensure that the data are trustworthy, confidential and reliable.
- **C13. Compliance with legislative requirements.** All patients and Health organizations are required to comply with relevant legislation to which they are subject. This includes prescribed laws, regulations and by-laws for Health.
- **C14. Using DLP Data Loss Prevention Tools-software:** These tools are used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users

The Critical Requirements associated with the aforementioned threats of Category D (Technology) for Cloud-based health system are the following:

- **D1. Bugs in large-scale distributed cloud systems:** Unfortunately, guaranteeing Cloud services' dependability is challenging because these cloud services are supported by large distributed systems such as scalable data stores, data-parallel frameworks and cluster management systems.

- **D2. Support heterogeneous devices and networks:** a Cloud-based health system can support highly heterogeneous devices, as well as can provide interoperability and communication through the hospitals and the systems.
- **D3. Vendor lock-in:** is the result of proprietary technologies that are incompatible with those of competitors. It is the situation where patients are dependent on a single Cloud Provider implementation and cannot easily move in the future to a different vendor without costs, legal constraints, or technical incompatibilities
- **D4. Isolation failure:** Multi-tenancy and shared resources are essential characteristics of Cloud Computing. This risk category covers the failure of mechanisms separating storage, memory, routing, and even reputation between different tenants.
- **D5. Prohibition against cross border transfer:** In globalized world, there are large amounts of cross-border transfers of health data, which are sometimes stored on servers in different countries.
- **D6. Authentication and Trust** Cloud-based Health systems require extensive authentication and trust in their services.

5. Security Policy Rules for every Category of Threats

As described in numerous relevant publications, a common practice to minimize the risk is to understand the internal control environment of a Cloud Provider and to analyze all the aspects, so we could identify possible contributing factors risks, including the definition of mitigation strategies. This is exactly what we present in our study. The proposed Methodology (Fig. 5) of our Security Policy can fulfill the entire list of Security Requirements of every Category of Threats that are covered by the following Security Policy Rules and provisions of our Cloud Security Policy Methodology.

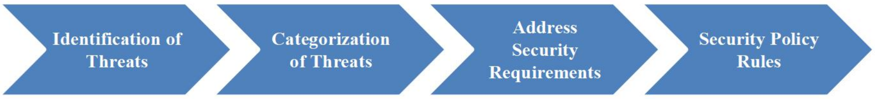
Identification of Threats
Categorization of Threats
Address Security Requirements
Security Policy Rules

Fig. 5. Processing of our Security Policy (Methodology)

Based on our analysis of threats in Cloud and the requirements related to these categories of threats, we have identified a number of security policy rules that make the integration of requirements into the development stages of a software systems development methodology considering Cloud-based Health System. These are the following tables (**Tables 1, 2, 3, 4)**

Table 1. Security Policy Rules specific for the Requirements of Category A

• **Security management:** should be based on risk assessment and should be active, surrounding all levels of participants' actions and operations.

- **Continual Reassessment**: making of suitable modifications to security policies, performs, measures and procedures.
- **Risk assessment:** should be adequately broad-based to include key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications.
- **Security Incidents Handling:** It is necessary to have the appropriate policies and procedures in order to handle effectively a range of security incidents.
- **Methods to Control Access:** the level of protection, the associated costs and the level of inconvenience that each option provides must be considered.
- **Technical measures for access control:** is based on the security that the physical barriers offer along with some additional means that permit access (a key).
- **Identifying Physical Assets:** The term includes the buildings, rooms, equipment a Cloud Provider is using.
- **Threat and vulnerability assessment:** Risk analysis method will reveal the potential threats against facilities, employees and clients.
- **Biometrics**: Biometric devices can provide some assurance that the person requesting entry is not using someone else's electronic access card or code.
- **Third Party:** Third party audits should be performed to monitor the Cloud Service Provider's compliance to agreed terms.

Table 2. Security Policy Rules specific for the Requirements of Category B

- **Personnel security:** It is essential for the protection of information assets, especially since information systems and services are operated by people.
- **Awareness:** Is the first line of Defense for the security of Information Systems, including their information assets, computing and communication systems.
- **Responsibility:** All contributors are responsible for the security of information systems and networks. They should be responsible to their individual roles
- **Response**: Participants should act in a timely and co-operative way to avoid, detect and respond to security incidents, recognizing the interconnectivity of information systems/ networks and the potential for fast and widespread damage.
- **Security Organizational Structure:** Organization should adopt the appropriate security organizational structure with the appropriate roles and suitably trained staff in order to support the security policy.
- **On-going staff education, Security Culture and Education:** Organizations shall ensure that employees are properly informed about their rights, obligations and security policies and that they accept their security responsibilities.
- **Continuous Monitoring:** Organization shall ensure that information contained in employee records is up-to-date by establishing the necessary procedures, in accordance to the Public Service Law and relative regulations.

Table 3. Security Policy Rules for the Requirements of Category C

- **Ethics:** Participants should respect the legitimate interests of others. They need to recognize that their action or inaction may damage others.
- **Categorized of Data:** Data should be categorized (Top Secret, Confidential, Sensitive, Reportable) in accordance with the protection they need, as this identified through the risk assessment or the assessment of the SP controller.
- **Localization of data**: In Cloud Computing data travels over the Internet to and from one or more regions where the data centers are. The user of Cloud must know: where the data are located, how the data are processed and by whom etc.
- **Identify the data sources, flow and destination:** This process must include data discovery and data fingerprinting that provides a better understanding, who, where, when and in what format the information is being generated.
- **Control Data:** In the absence of control data in a Cloud, no activity is recorded which modify or delete user's data. User should know how data is handled.
- **Using DLP data loss prevention tool-software:** is a strategy for making sure that end users do not sent sensitive or critical information outside the corporate network and prevent them by monitoring and detecting
- **Security Data Management:** When an outside party owns and manages resources, users should be assured that data remain private, secure and that the provider offers strong key management.
- **Conformance to Technical Standards:** Provide specialized expertise on relevant National and International technical standards such as: ISO/IEC 27000 Series of standards, NIST SP 800 standards, ETSI Security Standards.

Table 4. Security Policy Rules for the Requirements of Category D

- **Security design and implementation**: Security shall be a fundamental element of all products, services, systems and networks. A major focus of this effort is the design and adoption of appropriate safeguards and solutions.
- **General Configuration Guidelines:** Operating System configuration should be in accordance with approved Information Security guidelines.
- **Monitoring:** All security-related events on sensitive systems shall be logged and audit trails saved as follows: logs will be kept online for a minimum of 1 week. Daily incremental tape backups will be retained for at least 1 month. Weekly full tape backups of logs will be retained for at least 1 month. Monthly full backups will be retained for a minimum of 2 years.
- **Compliance:** Audits will be performed on a regular basis by authorized Organisations within the Cloud Provider and will be managed by the internal audit teams. Every determination will be made to stop audits from causing failures.
- **Malware Protection**: Never download files from unknown or suspicious sources. Never install unauthorized programs or applications. Choose and issue

default anti-malware/anti-virus software.

- **Security of Software**: Changes to the software are approved prior to their implementation. Changes that affect - directly or indirectly.
- **Portable Computing:** Portable information assets shall be adequately protected wherever they are used, whilst being transported or stored and when being disposed of Provider’s IT equipment shall only be used by authorized users.

6. Conclusions

In this paper, we presented a list of some basic security requirements and security policy rules for the deployment of Cloud-based Health System in an SaaS Cloud environment. Based on our analysis of the security and privacy threats in the Cloud and the categorization of these threats, we acknowledged an amount of security policy requirements and security policy rules that fulfill the provisions of every category of threats. Finally, we presented a proposed Model that provides a solution to the security challenges of Cloud Computing. The focus of this research, is, to minimize the risks that are presented in a Cloud-based health system and to present a Framework that offers the appropriate security to patients’ data and achieves the required assurance level of protection. The proposed Cloud Model Service improves the security and integrity of the medical records without affecting data access functionality from a user perspective. Given the dynamic development in the area of Cloud Computing, the security recommended policy rules listed above, need to be regularly reviewed and adjusted, and additional requirements may need to be added.

We must keep in mind that, in order to address the challenges all parties involved need to work together to create uniform and interoperable solutions that will allow a better Cloud-based health System to exist. We believe priorities in e-Health may be mentioned as a national issue, so we hope this contribution will encourage an exchange of best practices and lessons learned in migrating public e-health systems to fully virtualized SaaS Cloud-based environments.

Acknowledgment

This research is co-financed by Greece and the European Union (European Social Fund- ESF) through the Operational Programme «Human Resources Development, Education and Lifelong Learning» in the context of the project “Reinforcement of Postdoctoral Researchers - 2nd Cycle” (MIS-5033021), implemented by the State Scholarships Foundation (IKY).

Ευρωπαϊκή Ένωση
European Social Fund

Operational Programme
Human Resources Development,
Education and Lifelong Learning
Co-financed by Greece and the European Union

ΕΣΠΑ
2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

References

1. L.Goodwin, K, Courtney. D. Kirby, K. and M.A. Iannacchione and T.Manley (2002) : A pilot study: Patients' perceptions about the privacy of their medical records. Online Journal of Nursing Informatics,, 6(3).
2. Flynn, H., Marcus, S., Kerber, K. and Alessi, N. (2003) : Patients' Concerns About and Perceptions of Electronic Psychiatric Records. Psychiatric Services, 54(11), pp.1539-1541.
3. Silber, D. (2003), http://www.openclinical.org/e-Health, last accessed 2018/11/9.
4. Han, Song & Skinner, Geoff & Potdar, Vidyasagar & Chang, Elizabeth. (2006): A framework of authentication and authorization for e-health services. 105-106. doi: 10.1145/1180367.1180387.
5. H. Oh, C. Rizo, M. Enkin, and A. Jadad,: What is eHealth (3): a systematic review of published definitions, In: Journal of medical Internet research, vol. 7, no. 1, (2005).
6. R.E. Scott, M.F.U. Chowdhury, S. Varghese.: Telehealth policy: looking for global complementarity, Telemed. Telecare 8 (2002) 55—57.
7. Gematik - gesellschaft fur telematikanwendungen der gesundheitskarte. : http://www.gematik.de, last accessed 2017/11/27.
8. C. Chatman.: How cloud computing is changing the face of health care information technology. Journal Health Care Compliance, vol. 12, pp. 37–70 (2010)
9. J. T. Dudley, Y. Pouliot, R. Chen, A et al, 'Translational bioinformatics in the Cloud: an affordable alternative', vol. 2, p. 51, Genome Med (2010)
10. J. Kabachinski.: What's the forecast for Cloud Computing in healthcare?, Biomed Instrum Technol. 2011 Mar-Apr;45(2):146-50. doi: 10.2345/0899-8205-45.2.146
11. 1. Meingast M, Roosta T and Sastry S.: Security and privacy issues with health care information technology. In: Conference Proceedings IEEE Eng Med Biol Soc 2006; 1: 5453–5458.
12. Shmatikov V.: Anonymity is not privacy: technical perspective. Journal Communications of the ACM, 54: 132–132 (2011)
13. Reynolds B, Venkatanathan J, Gonçalves J et al :Sharing ephemeral information in online social networks: privacy perceptions and behaviors. In: 13th IFIP TC 13 International Conference on Human-computer interaction on Proceedings, pp. 204-215. (2011)
14. De Vimercati SDC, Foresti S, Livraga G et al: Protecting privacy in data release In: Aldini A and Gorrieri R (eds) FOSAD VI. Berlin: Springer, 2011, pp.1–34.
15. Georgiou D., Lambrinoudakis C. (2015) Cloud Computing Security Requirements and a Methodology for Their Auditing. In: Katsikas S., Sideridis A. (eds) E-Democracy – Citizen Rights in the World of the New Computing Paradigms. e-Democracy 2015. Communications in Computer and Information Science, vol 570. Springer, Cham
16. Georgiou D., Lambrinoudakis C.: Security policy rules and required procedures for two crucial cloud computing threats. International Journal of Electronic Governance,Vol.9 No.3/4, pp.385 - 403 (2017)
17. Georgiou D., Lambrinoudakis C:A Security Policy for Cloud Providers The Software-as-a-Service Model,Conference: ICIMP 2014 : The Ninth International Conference on Internet Monitoring and Protection
18. Final European progress report, E-health strategies : www.ehealth - stragies.eu/report/report.html, last accessed 10/11/2018
19. European Commission SWD (2012) 413 final. (2018).
20. Communication from the Commission to the Council the European Parliament ,the European Economic and Social Committee and the Committee of the Regions, COM(2004) 356: e-Health—making health care better for European citizens: an action plan for a European e-Health Area {SEC(2004) 539} Brussels: European Commission; 2004.

21. European Commission SWD (2012) 414 final. (2018): On the applicability of the existing EU legal framework to telemedicine services. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2012:0414:FIN:EN:PDF, last accessed 24/12/2018.
22. Action77: Foster EU-wide standards, interoperability testing and certification of e Health: digital Agenda for Europe: http://ec.europa.eu/digital-agenda/en/pillar-vii-ict-enabled-benefits-eu-society/action-77-foster-eu-wide-standards-interoperability last accessed 28/8/2018.
23. EU activities in the field of e Health interoperability and standardization: an overview' [press release]. (European Commission 2013)
24. Europe's Information Society eHealth portal http://europa.eu.int/information_society/activities/health, accessed 30/09/2019
25. European Commission. (2012). eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century: http://ec.europa.eu/health/ehealth/docs/com_2012_736_en.pdf, last accessed 12/12/2019
26. European Parliament, Council of the European Union. 'Decision on adopting a programme of Community action on health monitoring within the framework of action in the field of public health (1997–2001) (1400/97/EC)' Off J EurCommunities 1997;40:1–10.
27. European Parliament, Council of the European Union. 'Decision on adopting a programme of Community action in the field of public health (2003–2008) (1786/2002/EC)', Off J Eur Union 2002;45:1–11.
28. European Parliament, Council of the European Union. 'Decision on establishing a second programme of Community action in the field of health (2008–13) (1350/2007/EC)' Off J Eur Union 2007; 50:3–13.
29. eHealth Industries Innovation, 'What is e Health?' e Health Industries Innovation (ehi2) Centre, http://www.ehi2.swan.ac.uk/en/what-is-ehealth.htm. Last accessed 3/4/2014.
30. European Commission. (2012). eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century http://ec.europa.eu/health/ehealth/docs/com_2012_736_en.pdf, last accessed 12/12/ 2018
31. Khazaei H, Misic J, Misic V Performance analysis of cloud computing centers using M/G/m/m+r. queuing systems IEEE Trans Parallel Distributed Systems 2012, 23:5.
32. Wang L, von Laszewski G, Younge A et al 'Cloud computing: A perspective study' New Generation Comput 2010, 28: 137–146.
33. Kleinrock L: Queueing Systems: Theory, vol. 1. Wiley-Interscience, 1975.
34. Mao M, Li J, Humphrey M ' Cloud auto-scaling with deadline and budget constraints' In Grid Computing (GRID), 2010 11th IEEE/ACM International Conference; 2010:41–48.
35. Barham P, Dragovic B, Fraser K, et al ' Xen and the art of virtualization' SIGOPS Oper Syst Rev2003, 37(5): 164–177.
36. WMWare White paper http://www.vmware.com/pdf/virtualization.pdf, last accessed 25/11/ 2017.
37. The Open Stack Project: Open Stack 'The open source cloud operating system' http://www.openstack.org/software/, last accessed 30/11/ 2017
38. Mell P, Grance The NIST definition of cloud computing Gaithersburg: NIST Special Publication 800-145; 2011. 20899-8930.
39. Georgiou D.(2018) PhD Thesis Security Policies for Cloud Computing
40. Cloud Security Alliance, Top threats to Cloud Computing v1.0, https:// cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, last accessed 15/01/2019.
41. J. Heiser, M. Nicolett, Assessing the Security Risks of Cloud Computing, white paper, Gartner Group, 2008, ID Number: G00157782, last accessed 10/12/2018.