information

MDPI

Article

Compatibility of a Security Policy for a Cloud-Based Healthcare System with the EU General Data Protection Regulation (GDPR)

Dimitra Georgiou * and Costas Lambrinoudakis

Department of Digital Systems, University of Piraeus, 18534 Piraeus, Greece; clam@unipi.gr
* Correspondence: dimitrageorgiou@ssl-unipi.gr

Received: 27 October 2020; Accepted: 15 December 2020; Published: 17 December 2020

Abstract: Currently, there are several challenges that cloud-based healthcare systems around the world are facing. The most important issue is to ensure security and privacy, or in other words, to ensure the confidentiality, integrity, and availability of the data. Although the main provisions for data security and privacy were present in the former legal framework for the protection of personal data, the General Data Protection Regulation (GDPR) introduces new concepts and new requirements. In this paper, we present the main changes and the key challenges of the GDPR and, at the same time, we present how a cloud-based security policy could be modified in order to be compliant with the GDPR, as well as how cloud environments can assist developers to build secure and GDPR compliant cloud-based healthcare systems. The major concept of this paper is dual-purpose; primarily, to facilitate cloud providers in comprehending the framework of the new GDPR and secondly, to identify security measures and security policy rules, for the protection of sensitive data in a cloud-based healthcare system, following our risk-based security policy methodology that assesses the associated security risks and takes into account different requirements from patients, hospitals, and various other professional and organizational actors.

Keywords: cloud computing; healthcare systems; security; privacy; data protection; GDPR

1. Introduction

In the 21th century, since the adoption of the current data protection rules, people have altered their ways of communicating by using new channels to share their personal information, such as cloud computing. The fast expansion of information technology has exacerbated the need for strong personal data protection, the right to which is safeguarded by both the European Union and Council of Europe.

The EU General Data Protection Regulation 679/2016 [1] is the most noteworthy modification in data privacy over the last years. On 25 May 2018, it was fully enforced, revoking the current Data Protection Directive 95/46/EC [2].

The General Data Protection Regulation (GDPR) of the European Union (EU) addresses the protection of data subjects with regard to the processing and of their personal data. It introduces a set of rules across EU countries and citizens in order to secure their personal data. Most importantly, as a regulation and not a directive, it immediately becomes an enforceable law for all EU member states.

The GDPR requirements must be satisfied by all organizations that process and hold personal data of EU citizens, irrespective of being located within or outside the European Union. Thus, the GDPR affects all companies offering services to citizens residing in the EU, obliging them to comply with the new rules regardless of their location.

In order to understand the GDPR, first of all, we should describe the "personal data" that the GDPR protects.

Under EU law and according to the Council of Europe (CoE) Handbook [3], "personal data" are defined as information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Relating to an identified or identifiable natural person, that is, information about a person whose identity is either manifestly clear or can at least be established by obtaining additional information [4]. Therefore, the GDPR has expanded the personal data definition.

In addition, under the GDPR there are "special categories of personal data" which, by their nature, when processed, may put in jeopardy the data subjects and need enhanced protection. The GDPR refers to sensitive personal data as "special categories of personal data" in Article 9 [5] and therefore must be allowed only with specific safeguards. The types of data that fall into this category are "racial or ethnic origin, political opinions, religious beliefs, trade-union membership, genetic data, biometrics, concerning health, concerning sex life, related to criminal convictions".

The Data Protection Directive additionally lists "trade union membership" as sensitive data, as this information can be a strong indicator of political belief or affiliation. Convention 108 [6] also considers as sensitive personal data those linked to criminal convictions.

It is essential to underline that security, in the sense of integrity and confidentiality, is positioned at the heart of data protection together with the rest of the data protection principles, such as fairness and transparency, accuracy, and storage limitation, as security is considered to be one of the personal data processing principles in Article 5 of the GDPR [7].

More analytically, the scope of this paper is to facilitate cloud providers' understanding of how our risk-based approach for healthcare systems [8–10] can be utilized for building a secure and GDPR compliant environment. In addition, this study proposes possible security policy rules, pertaining to the protection of sensitive personal data, that are appropriate to the risk-based approach presented and that could be adopted by cloud providers, hospitals, other healthcare organizations, and clinical researchers for achieving compliance with the GDPR.

2. Overview of the Main Changes under GDPR

Numerous important observations linked to the security of personal data under the GDPR should be made. We identify the new elements introduced and we present the most important actions that cloud-based health organizations should take in order to comply with GDPR.

It is important to mention that security (in the sense of integrity and confidentiality) is established as one of the principles related to personal data processing, as presented in Article 5 of the GDPR [7].

The biggest change in the GDPR comes from the increased territorial scope of the GDPR. Whether the controllers and processors process the personal data in the EU or not, does not really matter as the requirements are applicable to each of them anyway. In Table 1, we present the key GDPR requirements, the rights of the data subjects, and a brief explanation.

The GDPR aims to address the growing risk through Article 5 and Article 32 [11], which set forth the basic rules for personal data processing by data controllers and processors.

Article 5 states "appropriate security of personal data should be ensured in the way data are processed", while Article 32 states "measures that would ensure an appropriate level of security, should be used by a data controller and processor when implementing a process to regularly test and assess the effectiveness of such security measures".

Table 1. Key changes of the General Data Protection Regulation (GDPR) [12].

	Key Changes of GDPR	Articles	Description
	Rights of the Data Subject		
1.	To data access	Article 15	Data subjects are entitled to know upon request at any time, what personal data a company is using, where and how it is being used, as well as for what purposes. With this right, data subjects will have more and clearer information and also access to data when they are collected for processing.
	To be informed	Article 13	This right provides the data subject with the ability to ask a company for information about what personal data are being processed and what the rationale is for such processing.
	Of rectification	Article 16	Data subjects have the right to require data controllers to rectify inaccurate personal data. Under the Data Protection Act (DPA), this principle is an obligation, not a subject's right, other than by court order. Organizations must reply to requests within one calendar month.
	To data erasure	Article 17	Data subjects have the right to request deletion of the personal data that concerns them, if they no longer wish the controller to hold the data.
	To restrict processing	Article 18	Data subjects have the right to require data controllers to restrict processing for the following reasons: • a data subject contests the accuracy of the data, the processing is unlawful, and a data subject opposes data erasure; • the data controller no longer needs the data but a data subject requires it to be kept for a legal claim; • a data subject has objected, pending verification of legitimate grounds.
	To data portability	Article 20	EU citizens have the right to transfer their personal data from one provider to another for processing. This right allows them to move, copy, and transfer personal data from one environment to another in an easy and secure way, but only when the processing is based on consent and the processing is automated.
	Not to be subject to automated decision making and profiling	Articles 22, 25 and 32	Data subjects have the right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her, or similarly significantly affects him or her". • This provision applies to the decision, not the execution of the automated processing to which the subject may object under Article 21. • Organizations involved in risk stratification or similar activities need to make sure that data subjects are given an opportunity to object before they are subject to decisions that meet the criteria.
	To object to the processing of their personal data	Article 21, 37, 38, 39	The controller must respect the objection unless they can demonstrate compelling legitimate grounds which override an individual's rights or for establishing, exercising, or defending legal rights. • In the case of processing for scientific or historical research or statistical purposes pursuant to Article 89(1), the right to object needs not to be respected where the processing is necessary for the performance of a task carried out for reasons of public interest.
2.	Increased territorial scope (extra territorial applicability), international Transfer of data, transfer of personal data to third countries of international organizations	Articles 44, 45, 46, 47, 48, 49, 50, 3	According to the GDPR, International companies that collect or process EU citizen data should comply with the GDPR. The GDPR is applicable to any entity controlling or processing the personal data of EU data subjects, regardless of where it operates. This means that any foreign company based outside of the EU member states that deals with the data of EU citizens is subject to the GDPR's stringent requirements.
3.	Data Protection Officer (DPO)	Articles 37, 38, 39	The GDPR introduces the role and the duties of the data protection officer (DPO) in Articles 37–40. Specific tasks of the DPO and corresponding obligations of the employers are presented there. In addition, it is stated that the contact details of the data protection officer should be made available to the public for ensuring uninterrupted communication with data subjects. It is an obligation for the controller and the processor to report to the supervisory authority the definition of the data protection officer.
4.	Breach Notification	Article 32, 33, 34	Organizations in all member states must report data breaches to supervisory authorities and individuals affected by a breach within 72 h (Article 33) of the detection. According to Article 34, a data subject should also be notified in the case where security breaches result in a risk to their rights and freedoms.

Table 1. *Cont.*

	Key Changes of GDPR	Articles	Description
5.	Data Protection Impact Assessment	Article 35	The GDPR makes it obligatory for a data protection impact assessment to be completed where the processing is likely to result in a high risk to the rights and freedoms of data subjects. • This is required in particular for some automated processing on which decisions concerning individuals are based, processing on a large scale of special categories of data (for example health or genetic data) or systematic monitoring of a public area (for example Closed Circuit Television (CCTV)). • There is a list of essential elements for completion of the assessment. • Where risks identified cannot be sufficiently addressed, the data controller must consult the Supervisory Authority.
6.	Penalties	Article 83, 84, 28	Under the GDPR legislation, organizations can get fined. There is a layered approach regarding fines. The lower level of fine, up to €10 million or 2% of the company's global annual turnover will be considered for infringements listed in Article 83 (4) of the GDPR. The higher level of fine, up to €20 million or 4% of the company's global annual turnover will be considered for infringements listed in Article 83 (5) of the GDPR.
7.	Consent Conditions for consent	Article 6, 7, 8 and 4(11)	Under the GDPR the conditions for consent have been strengthened. Terms and conditions should be presented in an easily accessible, understandable, and intelligible form by companies, with the purpose for data processing attached to that consent. Consent must use clear and plain language.
8.	Independent Supervisory Authorities	Articles 51–54	Data protection authorities are independent public authorities that supervise, through investigation, the application of the data protection law. There should be one in each EU member state and they are the main contact point for questions on data protection in the EU member state where the organization is based.
9.	Data Protection by Design and by default	Article 25	The GDPR requires that organizations incorporate technical and organizational measures to minimize the risk to the rights and freedoms of subjects in both the design and operation of data processing activities. • In particular, only personal data that are necessary for each specific purpose of processing should be processed. • It also specifically mentions data minimization and the application of, for example, pseudonymization to achieve this.
10.	Records of processing activities	Article 30	The GDPR requires data controllers and processors to maintain records of their processing activities. • This supports an organization's accountability and ability to demonstrate compliance, and supports information to incorporate into transparency information provided to subjects. • The information that must be included in these records is specified. • These obligations do not apply to an organization employing less than 250 people unless other conditions are met, such as the processing carries a high risk to the rights and freedoms of a data subject, or includes special categories, for example, health data.

To begin with the changes of the GDPR, it is important to understand everyone's role in GDPR compliance as presented in Figure 1. There are four roles identified in the EU data protection regulation, with their own obligations and rights under the GDPR. The following entities are tied to compliance:

Controller (organization)

The controller determines the purpose and means of processing the data and must have a specific reason for data processing, ensure the accuracy and protect the data, inform supervisory authority in the case of a breach, and prevent transfer to insecure processors.

Processor (cloud service)

The processor processes data on behalf of controllers and takes additional measures. The processor must protect and process the data only in the way specified by the controller, have a signed agreement, and erase data once services are terminated.

Data subject (employee or customer)

The data subject is an individual who can be identified, in a direct or indirect manner. Their rights include consent/opt out, access data, know where data are, how data are processed, where data are communicated, and request data erasure.

Supervisory authority (data protection authority)

The supervisory authority (data protection authority) is a public authority that bears the role of supervising and enforcing the GDPR for a member state.

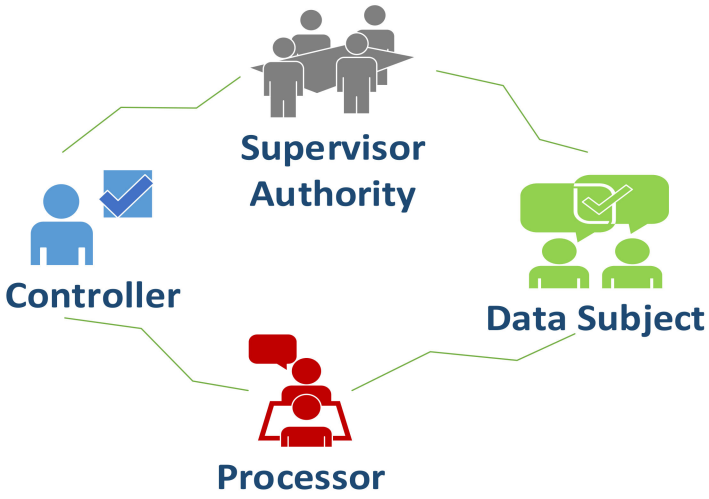

Figure 1. GDPR entities.

The key changes, introduced by the GDPR, with a brief explanation and a reference to specific articles, is provided in Table 2.

Table 2. Enhancement to the cloud-based security policy in order to be GDPR compliant.

GDPR Main Requirement Classes	Security Policy Rules Covered/Not Covered/ Partially Covered by the Security Policy Proposed in [1]	Links to the Security Policy Rules
Rights of data subjects	-	See Section 4.2.1 (A)
Increased territorial scope	○	See Section 4.2.2 (B)
Appoint a data protection officer	-	See Section 4.2.3 (C)
Breach notification	-	See Section 4.2.4 (D)
Privacy by design	•	See [1]
Data protection impact assessment	-	See Section 4.2.5 (E)
Penalties	-	See Section 4.2.6 (F)
Consent/conditions for consent	-	See Section 4.2.7 (G)
Independent supervisory authorities	-	See Section 4.2.8 (H)
Data protection by design and default	○	See [1] Section 4.2.9 (I)
Records of processing activities	•	See [1]

•, covered; -, not covered; ○, partially covered.

Cloud computing introduces a great number of compliance challenges to all GDPR entities. An important change is the introduction of the data processor role, for our purposes the cloud service provider, and its liabilities. Prior to the GDPR, the responsibility for data protection was that of the data owners and not that of the cloud service providers. From 28 May 2018, when the GDPR rules entered into force, the two have shared equal liability.

The complex architecture and the various specificities of healthcare systems, including the use of a cloud computing environment, imposes the need for organizations and providers to take additional measures in order to protect personal data.

The penalties for non-compliance are going to be huge and that is why it is really important for every organization to correctly understand the requirements and to be prepared.

The healthcare environment is undergoing fundamental changes under the GDPR, and therefore security is becoming a significant challenge for cloud-based healthcare systems [13] with the utmost importance [14]. The main data protection principles that a Software as a Service (SaaS) cloud computing provider will need to look at and be familiar with are depicted in Figure 2.

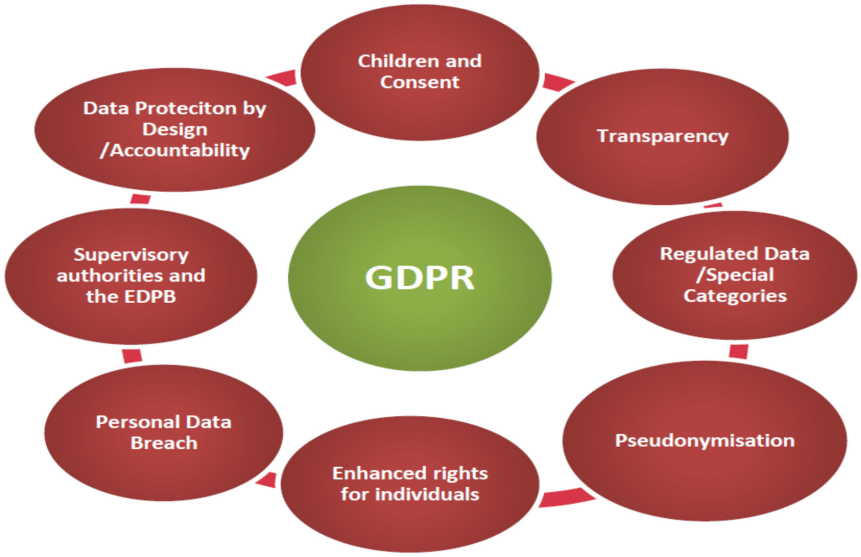

Figure 2. GDPR changes via the concepts.

3. Challenges of Cloud Adaptation in Healthcare Systems

Cloud computing is a recent and fast-growing area of development in the healthcare sector. The EU goals, in a healthcare environment, are to improve the health and wellbeing of populations, reduce health inequalities, strengthen public health, and to ensure sustainable people-centered healthcare systems that are universal, equitable, of high quality, and guided by good intersectoral governance. Clearly, information and communication technology in the healthcare sector plays a key role for expanding access to diagnostic services, improving their quality, increasing coordination between providers, improving patient management, and helping to overcome physical distances between patients and health professionals. For healthcare providers and patients, it is more convenient to have electronic health record applications and services over the cloud. Despite all the benefits of cloud computing, its adoption may lead to enormous security challenges that delay the migration of healthcare systems and data to the cloud, an issue needed to be carefully understood and considered.

Several studies have been conducted in the area of security for cloud computing on healthcare systems. For example, Mehraeen et al. presented in a systematic review the security challenges in cloud computing. They mainly focused on healthcare cloud computing security, with an organized review of 210 full text articles published. Their review of articles showed that for ensuring healthcare data security, it was important to provide authentication, authorization, and access control within

cloud's virtualized network. Issues such as identity management and access control, internet-based access, authentication and authorization, and cybercriminals were major concerns in healthcare cloud computing [15]. Zriqat et al. presented the Security and Privacy Issues in E-healthcare Systems: Towards Trusted Services. Through a systematic literature review, they presented existing security approaches and analyzed used security models [16]. P. D. G. Vyawahare et al. elaborated a survey on security challenges and solutions in cloud computing [17]. In this paper, the writers proposed a key policy advanced encryption standard associated with the user authorization period.

More analytically, Johnstone et al. [18] spoke about the integrity of data as a challenging task and reported that when users stored and transferred their healthcare information on the cloud they needed the assurance that the digital information was uncorrupted and could only be accessed or modified by those authorized to do so. Cheng et al. [19] mentioned the internet as another significant challenge in healthcare cloud computing and all the other security concerns that can happen related to the Internet, including frauds and attacks by hackers.

As an answer to these challenges, many researchers and practitioners have proposed several solutions to these challenges through their papers. Many have worked on identifying architectures, developing cloud-based healthcare applications and systems, presenting frameworks, strategies, and other security solutions (e.g., [20–24]).

Among various security challenges particularly faced by the e-Health Cloud SaaS systems, as identified by the related literature, the most important ones are the following:

Data/Service Reliability The use of cloud for e-Health systems poses the need for high reliability of the provided services. As such services are distributed, the chance of having faulty transmission or incorrect data can increase. The data in e-Health Cloud must be consistent and constantly in a valid state regardless of any software, hardware, or network failure.

Data Management/Control The data stored in a cloud virtualized environment can be accessed or managed through many people [25]. As such, in a healthcare cloud environment, the access control mechanisms employed for the protection of medical records are of vital importance [26]. The data may be replicated at different locations and across large geographic distances. Some of the data could be available locally. Most medical applications require secure, efficient, reliable, and scalable access to the medial records. The loss of direct data and application management can leave users feeling vulnerable to security flaws, data loss, and theft.

Cloud Security/Privacy Internet-based access is another challenge in healthcare cloud computing. The cloud service providers offer a large number of resources that are collected in a virtualized pool to be utilized by healthcare providers. Clouds are on the Internet, and thus data could be stolen by hackers for fraudulent purposes. Data security and privacy are the primary concerns for the healthcare industry. As the service becomes distributed in nature, the chances of erroneous data increases.

Data breach The most important thing is to prevent any data violation. Data can be comprised in in many different ways. A data breach in cloud is an incident involving unauthorized or illegal viewing, accessing or retrieval of data by an individual, application, or service. The aim is to steal and/or publish data to an unsecured or illegal location.

Despite the existence of several research works on the area of cloud computing security, we have also conducted research on the development of secure cloud-based healthcare information systems [27,28]. The development of a security framework for cloud-based healthcare information systems requires a full understanding of potential threats and challenges.

The steps employed during our research, have been the following:

Step 1 Review of existing studies on cloud computing security issues;
Step 2 Identify threats to cloud-based healthcare systems;
Step 3 Classify threats into distinct categories, i.e.,gates;
Step 4 Address security requirements based on identified threats and challenges;

Step 5 Determination of objectives in cloud-based healthcare systems;
Step 6 Determination of assets in cloud-based healthcare systems;
Step 7 Define security policy rules and procedures.

According to the results of our previous research work, the most important threats present in cloud-based computing environments are presented in [9–11]. The threats related specifically to cloud-based health information systems are also presented in [27,29–31]. The identified threats have been classified into the following distinct categories:

1. Identity and Access Management, i.e., the threats associated with inappropriate access of cloud computing resources.
2. Data, i.e., the threats associated with loss, leakage or unavailability of data.
3. Regulatory, i.e., the threats associated with non-compliance to various governmental, national/geographic regulations or legal and regulatory requirements.
4. Operational, i.e., the threats associated with the execution of business activities and services.
5. Technology, i.e., the threats associated with evolving technologies and lack of standardization.

In order to achieve an adequate level of protection in a SaaS cloud-based healthcare system, a risk assessment study was performed and the resulting security requirements (specifically for every category of threats) have been addressed through the appropriate security control and the appropriate security policy rules and procedures. The full security policy can be found in [28]. In the following section, we assess if the proposed security policy covers the main GDPR requirement classes (presented in Table 1). In the cases where the existing security policy [28] does not cover, or partially covers, the GDPR requirements, new policy rules are being proposed.

4. Results

4.1. Compliance of Our Security Policy Methodology with GDPR

In this section, the security policy for cloud-based healthcare information systems proposed in [28], is extended (Figure 3) in order to cover the GDPR provisions of Table 1.

In Table 2 we present the practical implications of the GDPR and how they are covered, or not covered, by our cloud security policy. For the requirements that are covered by the existing security policy, new security policy rules are proposed.

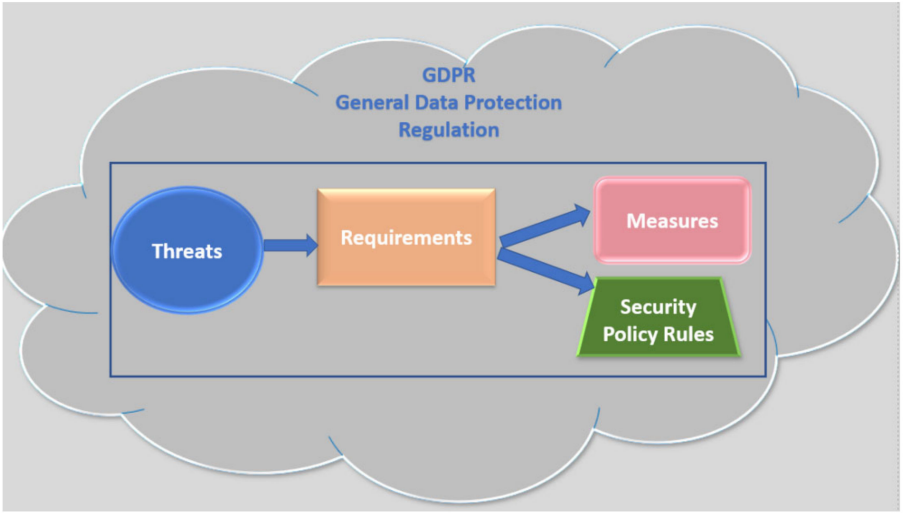

Figure 3. Overall methodology of a cloud-based security policy compliant with the GDPR.

This table aims to generate value for the healthcare organizations and providers with the scope to improve their care services at all levels, to promote data security and privacy across Europe, and to serve business growth in the field of cloud computing. To be compliant with the GDPR, as well as to safeguard the fundamental rights and freedoms of patients, there are some steps healthcare organizations should take to benchmark their current compliance. Therefore, based on the previous table, the GDPR implications that are not covered in our cloud security policy, are explicitly presented below with new security policy rules.

4.2. New Security Policy Rules

4.2.1. Rights of Data Subjects

In order for cloud-based health organizations and providers to be able to manage the requests of data subjects who use their services, concerning the exercise of their rights, we propose a specific procedure (Figure 4) that cloud-based healthcare organizations and providers should follow which includes identifying the details of data subjects, evaluating their requests, and deciding whether to satisfy them or not, while also informing them. The steps in the procedure are as follows:

Step 1 Collection of a data subject's request

The communication channels that a cloud-based healthcare organization supports, and the data subjects can use, in order to the exercise their rights are as follows:

- Physical presence, i.e., the data subject completes a standardized form on the premises of the cloud-based healthcare organization.
- Website, i.e., the data subject, after visiting the website of the cloud-based healthcare organization, completes the online form for exercising the data subject's rights.
- Mail (physical or electronic), i.e., the data subject can exercise one of their rights by writing a free text and sending it to the cloud-based healthcare organization via mail (postal address) or via e-mail.

Step 2 Identification and information of the data subject for the reception of the request

Upon receiving a request, the department/person who is responsible to receive it, must, within a reasonable time, proceed to identify the data subject who filed the request and to update the provided communication data in the case that the request has been submitted through the standard form. Therefore, the department is responsible for conducting any controls required to identify the subject.

The minimum required information for the identity of the data subject is the following:

- For the communication channel physical presence, identity card and passport, etc.
- For the communication channel website, phone communication and identification based on the existing identification process via phone.
- For the communication channel mail (postal address or e-mail), phone communication and identification based on the existing identification process via phone.

At the same time, the same department that receives the request of the data subject, informs the data subject that the request has been successfully received and the assessment process has begun. This action is necessary to effectively monitor the timeframe, to serve the request, and to avoid unjustified delays. It is noted that once the data subject has been identified, the cloud-based healthcare organization must manage the request and respond within thirty (30) days, with the possibility of extending an additional sixty (60) days. In the case that it is not possible to verify the identity of the data subject by the cloud-based healthcare organization, according to the above table, then, the data subject's request may be rejected. The process continues to Step 3.

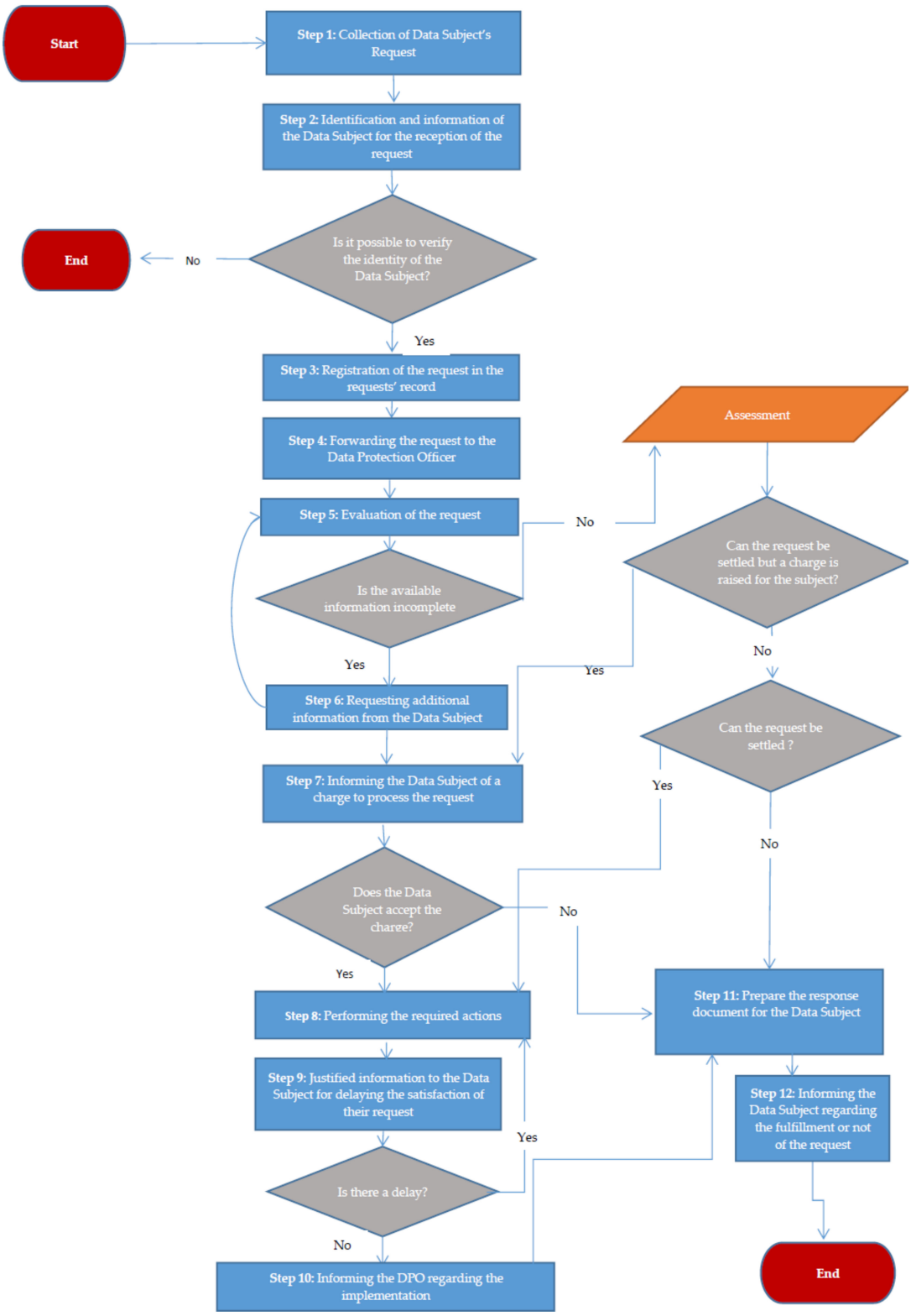

Figure 4. Process to satisfy the rights of data subjects.

Step 3 Registration of the request in the requests' record

Afterwards, the department/responsible person who received the request of the data subject, registers it in the "requests record". In this file (e.g., Excel, application), all requests that the cloud-based healthcare organization has received concerning the rights of the data subjects are recorded.

For each request, the following information must be recorded:

- Identification of the data subject (identity card, passport, driving license, etc.) unless a third party acts on behalf of the data subject;
- The type of exercised right (right of access, right of rectification, erasure, etc.);
- The channel through which cloud-based health organization received the request of the data subject;
- If the data subject wishes to receive the answer to its request through a specific communication channel;
- Useful details and information about the request of the data subject;
- If the data subject's request has been assessed as excessive or without appropriate legal basis/grounds, the reasons that led to this result;
- The date of receipt of the request by the responsible department of cloud-based healthcare organization;
- The date the data subject was identified;
- The date of the response by cloud-based healthcare organization;
- The channel through which the response was sent to the data subject.

The "requests record" is constantly updated as the above information is completed throughout this procedure. The process continues to Step 4.

Step 4 Forwarding the request to the data protection officer

All requests of the data subjects, regardless of the channel through which they were submitted and of the department/person who was responsible for receiving it, must be sent to the data protection officer. Therefore, any department of the cloud-based healthcare organization that receives a request regarding the rights of the subject must forward it to the data protection officer, so that an assessment is carried out and necessary further actions are taken. The procedure continues to Step 5.

Step 5 Evaluation of the request

At this stage of the process, the data protection officer, upon receipt of the request of the data subject, is responsible for thoroughly assessing the request to decide whether to proceed with its satisfaction. After analyzing all the available information, the data protection officer assesses whether the information is sufficient or whether additional information is needed from the data subject in order to assess the request effectively.

If the available information is considered to be incomplete and additional information from the data subject is required, the procedure continues to Step 6.

Otherwise, if the information held by the data protection officer in their possession is sufficient, they are in a position to proceed with an effective assessment of the data subject's request. An integral part of the assessment of the request is the identification of the relevant departments, which should be informed afterwards. Furthermore, for this assessment, the data protection officer should among others, seek the necessary information through the available information systems and/or get in contact with the departments of the cloud-based healthcare organization that may be related to the request of the data subject.

In addition, the processing activities record, where all personal data processing activities for which the cloud-based healthcare organization is responsible are recorded, can be used as a basis for the evaluation, as it provides the data protection officer with important information such as the following:

- The purpose of processing the data;
- The recipients of the data inside and outside of the cloud-based healthcare organization;
- The legal basis for processing the data;

- The information systems involved in the processing of such data;
- Having this information, the data protection officer can effectively assess the subject's request regarding the data subject's rights and classify the request as "request can be settled", "request can be settled but the subject is requested to pay a charge", or "request cannot be settled".

In Table 3, an indicative guide is presented concerning the assessment of a request.

Table 3. Request assessment table.

Request Assessment Table		
Request	**Description**	**Examples of Requests**
Request can be settled	Request that can be implemented within the foreseen timeframe (30 days).	Data rectification Data access Limitation of data processing
Request can be settled but the subject is requested to pay a charge	Request that is excessive (e.g., due to its repetitive character).	Multiple copies of data (X times over Y months)
Request cannot be settled	Unjustified request or request that is excessive (e.g., due to its repetitive character).	The subject has access to their data, but this will result in the disclosure of personal data of a third party. The subject has exercised the right to the portability of their data but has previously requested the erasure of the data.

If the request is assessed as "request can be settled but the subject is requested to pay a charge", the procedure continues to Step 7 of this procedure. If the data subject's request is assessed as "request can be settled", the process continues to Step 8. Finally, if the request is assessed as "request cannot be settled", the procedure continues to Step 11 of the procedure.

In any case, the data protection officer informs the responsible departments of the cloud-based healthcare organization in order to proceed to the necessary actions and/or updates based on the procedure.

Step 6 Requesting additional information from the data subject

If the available information when assessing the request is incomplete, then the department responsible in the Cloud-based Health Organization requests additional information from the data subject. Once the data subject provides the necessary information, the procedure continues to Step 5.

Step 7 Informing the data subject of a charge to process the request

The department responsible in the cloud-based healthcare organization informs the data subject that their request will be processed only if they pay a reasonable amount corresponding to the complexity of their request. If the data subject accepts the charge, the process continues to Step 8. Otherwise, the procedure continues to Step 11.

Step 8 Performing the required actions

The cloud-based healthcare organization must be able to satisfy the rights of the data subjects. Depending on the option(s) that the cloud-based healthcare organization defines, the data protection officer is able to communicate with the data subject via printed or electronic media.

One form for exercising data subjects' rights must be available both in printed form at the cloud-based healthcare organization's infrastructure and in an electronic form on its website. Alternatively, or complementarily, an e-mail account may be used by data subjects in order to submit their requests to the cloud-based healthcare organization for exercising their rights.

In order to satisfy the right to information and access, the cloud-based healthcare organization may use one document as a response template. In order to satisfy the rights of rectification, erasure, objection, limitation of processing, and data portability, the cloud-based healthcare organization, in cooperation with the data protection officer, should develop technical mechanisms to support these requests.

The cloud-based healthcare organization should maintain a "requests record" where details of how each data subject's request has been satisfied can be found.

The cloud-based healthcare organization may communicate responses to requests from data subjects by letter, either in a printed form or electronically, either via phone or via fax, if the natural person has been identified.

Step 9 Justified information to the data subject for delaying the satisfaction of their request

The department responsible, in the case that the data subject's request cannot be satisfied by the cloud-based healthcare organization, is responsible for informing the data subject within the period of thirty (30) days specified by the GDPR. This update must contain documented reasons regarding the delay of the satisfaction of the data subject's request. In order to gather documented information, the data protection officer must continuously monitor the process and the actions regarding the satisfaction of the data subject's request, in order to ensure that the request is satisfied promptly by the cloud-based healthcare organization. It is noted that the data subject can be informed regarding the delay of the satisfaction of his/her request, if necessary, later during this process. The procedure continues to Step 10.

Step 10 Informing the DPO regarding the implementation

Once the department or departments responsible have completed all the required actions for the satisfaction of the data subject's request, they must inform the data protection officer that the request has been served and that no further actions are required from their part. The procedure continues to Step 11.

Step 11 Prepare the response document for the data subject

The data protection officer must analyze all available information, whether the source is the data subject or deriving from the actions of the department(s) responsible in the cloud-based healthcare organization, and prepare the response to the data subject. These actions are carried out in any case, i.e., fulfillment of the request or not. In any case, the answer given to the data subject regarding the fulfillment or not of the request must be documented. The procedure continues to Step 12.

Step 12 Informing the data subject regarding the fulfillment or not of the request

The responsible department of the cloud-based healthcare organization must inform the data subject, appropriately, for the fulfillment or not of their request.

Therefore, the response to the data subject is communicated by the responsible department to the data subject via the selected communication channel as follows:

- By letter to the designated postal address of the data subject;
- Electronically, either if the data subject has requested so or if the request has been submitted by electronic means;
- Orally, if the data subject has requested so.

Finally, the responsible department updates the requests record, so that the request is properly marked as fulfilled. It is noted that this record proves that the data subject's request has been investigated promptly and the necessary actions have been taken and that the cloud-based healthcare organization has complied with the relevant GDPR requirements. The procedure is completed.

4.2.2. Increased Territorial Scope

In order to be able to manage the increased territorial scope, cloud-based healthcare organizations and providers should adopt the following security policies:

PR1 Appropriate safeguards must be taken, if personal data are stored outside the EEA.
PR2 Review data flows to ensure that appropriate transfer mechanisms are in place.
PR3 Choose a transfer mechanism, such as binding corporate rules (BCRs), standard contractual clauses (SCCs), privacy shields (for the USA).
PR4 If activities are in more member states, the provider should propose the state of the main establishment, the country that is the main residence of the provider.
PR5 Define a cloud strategy to adhere to sufficient requirements and data localization laws of a lot of countries' operations may have to be audited before the transfer is made.
PR6 Binding corporate rules (BCRs) as new appropriate safeguards should be taken.

4.2.3. Appoint a Data Protection Officer

Cloud-based healthcare organizations and providers should have a data protection officer (DPO) and should adopt the following security policies:

PR1 Review the current job specification of the organization's DPO.
PR2 The DPO should report directly to the board, have independence, and have a separate budget.
PR3 Depending on the size of the organization, consider whether the DPO is to require a support team to meet all the obligations of the GDPR.
PR4 Monitor and enforce the applicability of the GDPR.
PR5 Promote awareness and comprehension of the risks to the staff in the organization. In addition, inform the patients for their rights according the GDPR.
PR6 Data protection certification mechanisms should be established.
PR7 For liability, the data controller takes all appropriate security measures to protect personal data with liable way and in compliance with the regulation.
PR8 Specific attention should be addressed to children and their data.
RP9 The data processor must set appropriate technical and organizational measures to ensure an appropriate level of security.
PR10 The data controller has the obligation to inform the authority and the client as long as the breach poses a serious risk.
PR11 Codes of ethics are encouraged to be drawn up by the controllers, which are submitted for approval to the supervisory authority. In the case of trans-European activity, the European Data Protection Council is also consulted.

4.2.4. Breach Notification

In order to be able to manage the breach notification, cloud-based healthcare organizations and providers should adopt the following security policies:

PR1 Ensure clear security policies to avoid security breaches.
PR2 Deploy security controls that could help prevent security attacks.
PR3 Establish clear processes that enable reacting quickly to possible breaches.
PR4 Consider implementing security solutions that can detect, alert, and report on security breaches.
PR5 Monitor and report systematically how users who have access to personal data behave.
PR6 Breach notification obligations and protocols must be included in data processing agreements with cloud providers.
PR7 Review data breach policies.

PR8 Ensure security policies to notify the data subject when a data breach incident happens.

PR9 Notify the national authority within 72 h in the case of a data breach.

4.2.5. Data Protection Impact Assessment

In order to be able to manage the data protection impact assessment, cloud-based healthcare organizations and providers should adopt the following security policies:

PR1 Keep and document all information of data processing, such as what personal data are collected, as well as how data are protected, used, and stored.

PR2 Monitor and report in a file any unauthorized or illegal access attempts.

PR3 Monitor specific activities such as who accesses personal data and with whom the data are being shared.

PR4 Keep a record of how long the data are to be stored.

PR5 Ensure the data are encrypted, in order to protect it from any unauthorized access.

PR6 Prepare a template PIA and train relevant employees about how and when it should be used.

PR7 Ensure that outcomes and compliance steps are documented and actioned.

PR8 Check if your organization carries out activities other than the processing of health data that would require a PIA, for example, through the use of CCTV or health monitoring devices.

PR9 Adopt standards and show compliance through certification. In the case of cloud-based healthcare systems, the components should be compliant to industry standards GDPR or to acquire a security certification.

PR10 Perform a security assessment.

PR11 All systems should be commissioned and built using data protection by design and by default.

PR12 The IT and commissioning teams should be aware of the requirements of data protection by design and default.

PR13 Implementation of data-minimizing mechanisms.

PR14 Appropriate privacy protection measures have to be implemented.

4.2.6. Penalties

In order to be able to manage the penalties, cloud-based healthcare organizations and providers should adopt the following security policies:

PR1 If the cloud-based healthcare organization supplies services for EU-based citizens, the organization needs to comply with the requirements of GDPR.

PR2 Update and revisit the security policies in order to take the suitable steps for the protection of personal data.

PR3 Keep proper privacy documents that can be used to get explicit and clear consent from individuals to process their personal data.

PR4 Monitor the technical and organizational measures taken to ensure the privacy and security of personal data collected.

4.2.7. Consent/Conditions for Consent

In order to be able to manage the conditions for consent, cloud-based healthcare organizations and providers should adopt the following security policies:

SP1 The data subject's consent is required for personal data usage.

SP2 Specific and clear instructions for consent, to provide the legal basis for processing.

SP3 Provide separate consent options for each type of processing.

SP4 Create a common method to record consent.

SP5 Review the consents and identify who will carry out the review.
SP6 Identify the process for withdrawal.
SP7 Ensure data subjects are aware of the process for withdrawing their consent.

4.2.8. Independent Supervisory Authorities

Independent supervisory authorities should remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody. The main policy rules that they need are the following:

PR1 Performing tasks and exercising its powers in accordance with the regulation.
PR2 Review and approval of binding corporate rules (BCRs).
PR3 Use of approved certification mechanisms to demonstrate compliance with its requirements.

4.2.9. Data Protection by Design and Default

In order to be able to manage the data protection by design and default, cloud-based healthcare organizations and providers should adopt the following security policies:

PR1 Keep and document all information of data processing, such as what personal data are collected and how data are protected, used, and stored.
PR2 Monitor and report in a file any unauthorized or illegal access attempts.
PR3 Monitor specific activities such as who accesses personal data and with whom the data are being shared.
PR4 Keep a record of how long the data are to be stored, while being stored.
PR5 Ensure the data are encrypted, pseudonymized, and anonymized whenever possible, in order to protect them from any unauthorized access.
PR6 Adopt standards and show compliance through certification. In the case of cloud-based healthcare hospitals, the components should be in compliance with industry standards GDPR or acquire a security certification.
PR7 Perform a data protection impact assessment (DPIA) and a security assessment.
PR8 Define a control framework with privacy and privacy by design control measures in order to audit cloud provider.
PR9 The architecture of a cloud provider's system should be monitored to address any changes in technology.
PR10 Have a process in place to notify the authorities and your data subjects in the event of a data breach.
PR11 All new systems should be commissioned and built using data protection by design and by default.
PR12 The IT and commissioning teams should be aware of the requirements of data protection by design and default.
PR13 Implementation of data-minimizing mechanisms.
PR14 Appropriate privacy protection measures must be implemented.
PR15 Update the procedures for dealing with requests and the satisfaction of data subjects' rights, in particular as regards the deletion of data (right to forgotten) or the provision of them in a readable electronic format (data portability).
PR16 Inform the human resources about the upcoming changes, highlighting the significant impact in case of violations.
PR17 Assess the potential risks for the personal data collected and processed.
PR18 Develop a strategy for dealing with potential risks with technical and organizational measures.

5. Conclusions

This paper proposes a security policy for cloud-based healthcare information systems that satisfies the main requirements introduced by the GDPR. Furthermore, it allows stakeholders working with cloud-based healthcare data to acquire more awareness of data protection rules that allow EU citizens to have control over their personal data. The adoption of these security policy rules would enhance patients' trust since there is a secure cloud environment that guarantees patients' data are respected.

The policy issues, presented in this paper, are considered to be the basic issues pertaining to the GDPR in the healthcare cloud-based sector, but are not analytical and exhaustive. This research aims at providing practical advice and instruction to the EU cloud-based healthcare organizations to comply with GDPR, by helping them to assess and manage the risks for data protection, privacy, and other fundamental rights of individuals whose personal data are processed by cloud-based services [32]. Cloud service providers and healthcare organizations should define clear processes for maintaining security and privacy in cloud environments. Protecting sensitive medical data is one of the most essential responsibilities of healthcare organizations and one of the most tightly regulated in the cloud area [32].

In summary, this study identifies GDPR challenges that could emerge while adopting GDPR for private cloud-based healthcare systems. We present suggested security policy rules from the experience of designing a security policy for cloud systems, including issues of privacy requirements for private services on cloud computing.

Surely, a proper European cloud-based healthcare framework of a national nature is a prerequisite. This cloud security framework starts and ends with patients' needs. They are the owners of their data and they should know what benefit they will have from the GDPR in a cloud-based healthcare system and how much it could simplify their life and increase the quality of the service.

Author Contributions: Conceptualization, D.G. and C.L.; methodology, D.G. and C.L.; writing—original draft preparation, D.G.; writing—review and editing, D.G. and C.L.; supervision, C.L.; project administration, D.G. and C.L.; funding acquisition, D.G. and C.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been partly supported by the University of Piraeus Research Center. 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 (ΙΚΥ).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119. 4 May 2016. p. 1–88. Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 16 December 2020).
2. 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. Available online: https://eur-lex.europa.eu/eli/dir/1995/46/oj (accessed on 16 December 2020).
3. Council of Europe Handbook on European Data Protection Law 2018 Edition. Available online: https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (accessed on 16 December 2020).
4. Art. 4 GDPR—Definitions. Available online: https://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm (accessed on 16 December 2020).

5. Art. 9 GDPR Processing of Special Categories of Personal Data. Available online: https://gdpr-info.eu/art-9-gdpr/ (accessed on 16 December 2020).
6. Convention 108 + Convention for the Protection of Individuals with Regard to the Processing of Personal Data. Available online: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (accessed on 16 December 2020).
7. Art.5 GDPR—Principles Relating to Processing of Personal Data. Available online: https://www.privacy-regulation.eu/en/ (accessed on 16 December 2020).
8. Georgiou, D.; Lambrinoudakis, C. A Security Policy for Cloud Providers. In Proceedings of the 9th International Conference on Internet Monitoring and Protection (ICIMP 2014), Paris, France, 20–24 July 2014; pp. 13–21.
9. Georgiou, D.; Lambrinoudakis, C. Cloud Computing Security Requirements and a Methodology for Their Auditing. In Proceedings of the 2015 International Conference on e-Democracy, Athens, Greece, 10–11 December 2015; Springer: Cham, Switzerland, 2015; pp. 51–61.
10. Georgiou, D.; Lambrinoudakis, C. Security policy rules and required procedures for two crucial cloud computing threats. *Int. J. Electron. Gov.* **2017**, *9*, 385–403. [CrossRef]
11. Article 12 EU GDPR—Transparent Information, Communication and Modalities for the Exercise of the Rights of the Data Subject. Available online: https://www.privacy-regulation.eu/en/article-12-transparent-information-communication-and-modalities-for-the-exercise-of-the-rights-of-the-data-subject-GDPR.htm (accessed on 16 December 2020).
12. Information Governance Alliance "The Genera; Data Protection Regulation What's New". Available online: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance (accessed on 16 December 2020).
13. Wooten, R.; Klink, R.; Sinek, F.; Bai, Y.; Sharma, M. Design and Implementation of a secure Healthcare Social Cloud System. In Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, Ottawa, ON, Canada, 13–16 May 2012.
14. Wainer, J.; Campos, C.J.R.; Salinas, M.D.U.; Sigulem, D. Security Requirements for a Lifelong Electronic Health Record System: An Opinion. *Open Med. Inform. J.* **2018**, *2*, 160–165. [CrossRef] [PubMed]
15. Mehraeen, E.; Ghazisaeedi, M.; Farzi, J.; Mirshekari, S. Security Challenges in Healthcare Cloud Computing: A Systematic Review. *Glob. J. Health Sci.* **2016**, *9*, 59729. [CrossRef]
16. Zriqat, A. Security and Privacy Issues in Ehealthcare Systems: Towards Trusted Services. *Int. J. Adv. Comput. Sci. Appl.* **2016**, *7*, 229–236.
17. Vyawahare, P.D.G.; Bende, R.B.; Bhajipale, D.N.; Bharsakle, R.D.; Salve, A.G. A Survey on Security Challenges of Healthcare Analysis Over Cloud. *Intern. J. Eng. Res. Technol.* **2017**, *6*, 4069–4073.
18. Johnstone, M. Cloud security: A case study in telemedicine. In Proceedings of the 1st Australian e-Health Informatics and Security Conference, Perth, Australia, 3–5 December 2012.
19. Cheng, F.C.; Lai, W.H. The Impact of Cloud Computing Technology on Legal Infrastructure within Internet—Focusing on the Protection of Information Privacy. *Procedia Eng.* **2012**, *29*, 241–251. [CrossRef]
20. Alzoubaidi, A.R. Cloud Computing National e-health services: Data Center Solution Architecture. *Int. J. Comput. Sci. Netw. Secur.* **2016**, *16*, 1–6.
21. Plachkinova, M.; Alluhaidan, A.; Chatterjee, S. Health Records on the Cloud: A Security Framework. In Proceedings of the International Conference on Health Informatics and Medical Systems, Dallas, TX, USA, 27–30 July 2015; pp. 152–158.
22. Noufal, M.M. Smart e-Health Monitoring and Maintenance Using Cloud. *Int. J. Res. Emerg. Sci. Technol.* **2016**, *3*, 61–65.
23. Rani, A.A.V.; Baburaj, E. An Efficient Secure Authentication on Cloud Based e-Health Care System in WBAN. *Biomed. Res.* **2016**, 53–59. Available online: https://www.biomedres.info/biomedical-research/an-efficient-secure-authentication-on-cloud-based-ehealth-care-system-in-wban.html (accessed on 16 December 2020).
24. Dong, N.; Jonker, H.; Pang, J. Challenges in eHealth: From enabling to enforcing privacy. In *Foundations of Health Informatics Engineering and Systems*; FHIES, 2011; Lecture Notes in Computer, Science; Liu, Z., Wassyng, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 195–206.
25. Velumadhava, R.R.; Selvamani, K. Data Security Challenges and Its Solutions in Cloud Computing. *Procedia Comput. Sci.* **2015**, *48*, 204–209. [CrossRef]

26. Balasubramaniam, S.; Kavitha, V. Hybrid Security Architecture for Personal Health Record Transactions in Cloud Computing. *Adv. Inf. Sci. Serv. Sci.* **2015**, *7*, 121–130.
27. Georgiou, D.; Lambrinoudakis, C. Security and Privacy Issues for Intelligent Cloud-Based Health Systems. In *Advanced Computational Intelligence in Healthcare-7*; Studies in Computational Intelligence; Maglogiannis, I., Brahnam, S., Jain, L., Eds.; Springer: Berlin/Heidelberg, Germany, 2020; Volume 891. [CrossRef]
28. Dimitra, G. Security Policies for Cloud Computing. 2018. Available online: http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/11007/Georgiou_Dimitra.pdf?sequence=1&isAllowed=y (accessed on 16 December 2020).
29. Cloud Security Alliance. Top Threats to Cloud Computing: Deep Dive. 2018. Available online: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/top-threats-to-cloud-computing-deep-dive.pdf (accessed on 16 December 2020).
30. ENISA. Threat Landscape Report 2018 15 Top Cyber Threats and Trends. 2018. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (accessed on 16 December 2020).
31. ISACA. Security Considerations for Cloud Computing. 2012. Available online: https://www.isaca.org/bookstore/Pages/Product-Detail.aspx?Product_code=SCC (accessed on 16 December 2020).
32. European Data Protection Supervisor. Guidelines on the Use of Cloud Computing. 2018. Available online: https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf (accessed on 16 December 2020).