

Article

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

Dimitra Georgiou ^{1,*} and Costas Lambrinoudakis ²

¹ Department of Digital Systems, University of Piraeus, M. Karaoli & A. Dimitriou 80, 18534 Piraeus, Greece; dimitrageorgiou@ssl-unipi.gr

² Department of Digital Systems, University of Piraeus, M. Karaoli & A. Dimitriou 80, 18534 Piraeus, Greece; clam@unipi.gr

* Correspondence: dimitrageorgiou@ssl-unipi.gr;

Abstract: Currently, there are several challenges that Cloud-based health-care 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 General Data Protection Regulation, and also at the same time we present how the Cloud-based Security Policy methodology proposed in [1] could be modified in order to be compliant with the GDPR and how Cloud environments can assist developers to build secure and GDPR compliant Cloud-based health Systems. The major concept of this paper is, primarily, to facilitate Cloud Providers in comprehending the framework of the new General Data Protection Regulation and secondly, to identify security measures and security policy rules for the protection of sensitive data in a Cloud-based Health 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; Health Systems; Security, Privacy, Data Protection, GDPR

1. Introduction

In the 21st 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 European Union and Council of Europe.

The EU General Data Protection Regulation 679/2016 (GDPR) [2] 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 [3].

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 becomes immediately 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, GDPR affects all companies offering services to citizens residing in EU obliging them to comply with the new rules regardless of their location.

In order to understand the Data Protection Regulation, first of all, we should mention, what are the “personal data”, that GDPR protects.

Under EU law as well as under the Council of Europe (CoE) law [4], ‘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 [5]. So, GDPR has expanded the “personal data” definition.

In addition, under the General Data Protection Regulation 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 [6] and must therefore 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 [7] 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 in the heart of data protection together with the rest of data protection principles, such as fairness and transparency, accuracy and storage limitation, as it is considered one of the personal data processing principles in Article 5 of GDPR [8].

More analytically, the scope of this paper is to facilitate Cloud Providers understand how our risk based approach for health-care systems [9-11], 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, which are appropriate to the risk based approach presented and they could be adopted by Providers, hospitals, other health-care organizations and clinical researchers for achieving compliance with GDPR.

2. Overview of the main changes under GDPR

Numerous important observations linked to the security of Personal Data under 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 relating to personal data processing, as presented in Article 5 of GDPR [12].

The biggest change in GDPR comes from the increased territorial scope of the GDPR. Whether the controllers and processors will process the personal data in the EU or not, does not really matter

as the requirements will be applicable to each of them anyway. At the following table (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 [13], 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 is 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”.

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 Entities tied to compliance are:

2. Controller (Organization)

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

3. Processor (Cloud Service)

Processes data on behalf of controllers and take additional measures. Must protect, process the data only in the way specified by the controller, have a signed agreement and erase data once services are terminated.

4. Data Subject (Employee or Customer)

An individual who can be identified, in a direct or indirect manner. Rights include consent/opt out, access data, know where data is, how they are processed, where they are communicated and request data erasure.

5. Supervisory Authority (Data Protection Authority)

Public authority that bears the role of supervising and enforcing GDPR for a member state. The supervisory authority (Data Protection Authority or DPA) is the public authority that supervises and enforces the GDPR on its Member State's territory.

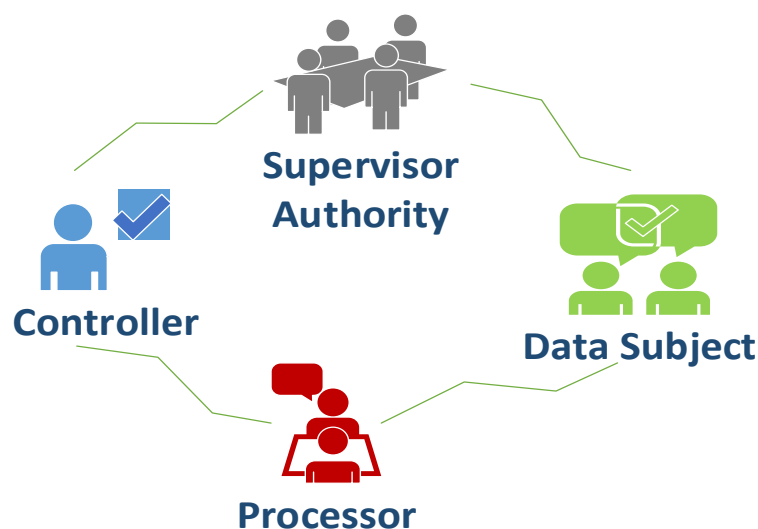


Figure 1 GDPR Entities

The key changes, introduced by the GDPR, with a brief explanation and a reference to specific Articles, is provided in the following table:

Table 1 GDPR key changes

	Key Changes of GDPR	Articles	Description
1	Rights of the Data Subject		
	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 (about him or her) is being processed and the rationale for such processing.
	to 'be forgotten' and to data erasure	Article 17	EU citizens can expect companies to stop processing and to delete their personal data upon request. They have the right to request r deletion of the personal data that concerns them, if they no longer wish the controller to hold them
	of rectification	Article 16	Data subjects have the right to require data controllers to rectify inaccurate personal data. Under the DPA, this is a principle obligation, not a subject right other than by court order. Organisations must reply to requests within one calendar month
	To restrict processing	Article 18	Data subjects have the right to require data controllers to restrict processing where: accuracy is contested by the data subject processing is unlawful and the subject opposes erasure the data controller no longer needs the data, but the subject requires it to be kept for legal claims the 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	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'. <ul style="list-style-type: none"> • This provision applies to the decision, not the execution of the automated processing to which the subject may object under Article 21. • Organisations involved in risk stratification or similar activities will need to make sure that 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 Data Protection Officer (DPO)	Article 21,37, 38, 39	<p>The controller must respect the objection unless they can demonstrate compelling legitimate grounds which override the individual's rights or for establishing, exercising or defending legal rights.</p> <ul style="list-style-type: none"> • In the case of processing for scientific or historical research or statistical purposes pursuant to Article 89(1), the right to object need not be respected where the processing is necessary for the performance of a task carried out for reasons of public interest. The GDPR introduces the role and the duties of the Data Protection Officer 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.
	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	<p>According to the GDPR, International companies that collect or process EU citizen data should comply with the GDPR.</p> <p>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 will be subject to the GDPR's stringent requirements.</p>
2.	Data Protection Officer (DPO)	Articles 37, 38, 39	<p>The GDPR introduces the role and the duties of the Data Protection Officer 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.</p>
3.	Breach Notification	Article 32,33, 34	<p>Organizations in all Member States must report data breaches to supervisory authorities and individuals affected by a breach within 72 hours (article 33) of the detection. According to article 34 a data subject should be also notified in case where security breaches result in a risk to their rights and freedoms.</p>
4.	Privacy by design	Article 25 and 32	<p>Companies should be in a position to provide a reasonable level of data protection and privacy to EU citizens. But, It's not clear what the GDPR governing body will consider reasonable. From the other side, the Controller should use</p>

			appropriate measures and use Privacy Enhancing Technologies such as aliasing personal data and encryption minimize data processing.
5.	Data Protection Impact Assessment	Article 35	<p>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.</p> <ul style="list-style-type: none"> • 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 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 ICO.
6.	Penalties	Article 83, 84, 28	Under 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 General Data Protection Regulation. 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 General Data Protection Regulation.
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, 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 investigative the application of the data protection law. There should be one in each EU Member State and will be 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 default	Article 25	<p>The GDPR requires that organisations 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.</p> <ul style="list-style-type: none"> • In particular, only personal data that is 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	<p>The GDPR requires data controllers and processors to maintain records of their processing activities.</p> <ul style="list-style-type: none"> • This supports an organization's accountability and ability to demonstrate compliance, and supports information to incorporate in transparency information provided to subjects. • The information that must be included in these records is specified.

			<ul style="list-style-type: none"> • 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.
--	--	--	---

The 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 Providers, and its liabilities. Prior to the General Data Protection Regulation, the responsibility for the data protection was of that data owners and not of the Cloud Services Providers. From the 28th of May 2018, when the GDPR rules entered into force, the two will share equal liability.

The complex architecture and the various specificities of Health-care systems, including the use of 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 understand correctly the requirements and to be prepared.

The health-care environment is undergoing fundamental changes under GDPR, turning security to a big challenge for Cloud-based health care systems [14] with utmost importance [15]. There main data protection principles that a Software as a Service (SaaS) Cloud Computing provider will need to look at and be familiar with are the following:

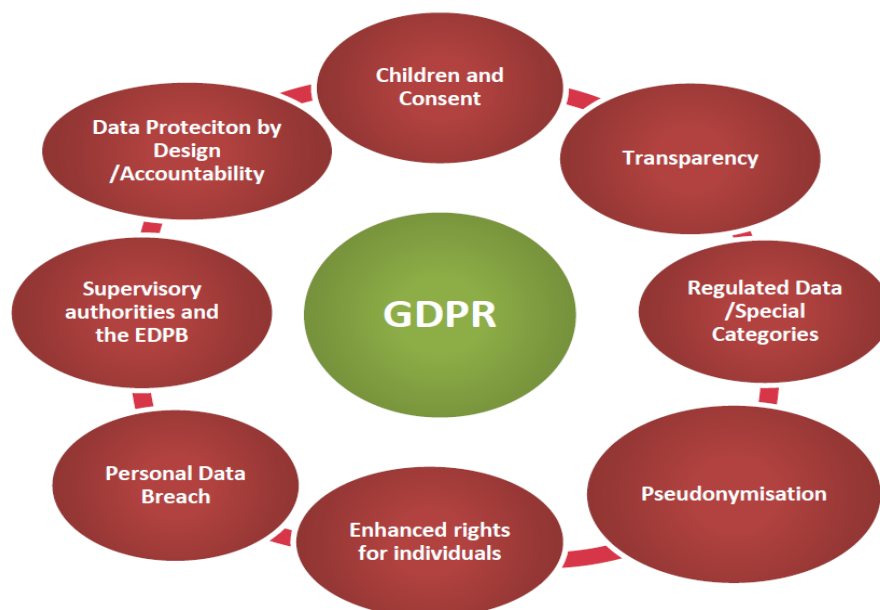


Figure 2 GDPR Changes via the concepts

3. Challenges of Cloud adaptation in Health systems

Cloud computing is a recent and fast growing area of development in health-care sector. The EU goals in Health-care environment, are to improve the health and well-being of populations, reduce health inequalities, strengthen public health and ensure sustainable people-centered health systems that are universal, equitable, of high quality and guided by good intersectoral governance. Clearly, Information and Communication Technology in health-care sector plays a key role in 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 health-care 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 Health 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 health care systems. Indicatively, Mehraeen et.al. presented in a systematic review the security challenges in Health-care Cloud Computing [17]. Zriqat et.al. presented the Security and Privacy Issues in E-healthcare Systems: Towards Trusted Services[18] P. D. G. Vyawahare et.al. elaborated A Survey on Security Challenges and Solutions in Cloud Computing [19].

More analytically, Johnstone et al.[20] spoke about the integrity of data, as a challenging task. When users store and transfer their health-care information on the cloud they need the assurance that digital information is uncorrupted and can only be accessed or modified by those authorized to do so. Cheng et al.[21], mentioned the internet as another significant challenge in health-care Cloud Computing and all the other security concerns related to Internet, including frauds and attacks by hackers, that may happen.

As an answer to these challenges, many researchers and practitioners proposed several solutions to these challenges through their papers. Plenty of them worked on identifying architectures, developing cloud-based health applications and systems, presenting frameworks, strategies and other security solutions (e.g. [22][23][24][25][26]).

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 cloud virtualized environment can be accessed or managed through many people [27]. As such in a health-care Cloud environment the access control mechanisms employed for the protection of medical records are of vital importance [28]. 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 medical records. The loss of direct data and applications management can leave users feeling vulnerable to security flaws, data loss, and theft.
- **Cloud Security/Privacy:** Internet-based access is another challenge in health-care Cloud Computing. The cloud service providers offer a large number of resources that are collected in a virtualized pool to be utilized by health-care providers. Clouds are on Internet, and thus, data might be stolen by hackers for fraudulent purpose. Data security and privacy are primary concerns for the health-care 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 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 Health information systems[1] and

[29]. The development of a security framework for cloud-based health services requires full understanding of potential threats and challenges.

The steps employed during our research, are the following:

- Step 1: Review of existing studies on Cloud Computing security issues
- Step 2: Threat Identification in Cloud-based Health Systems
- Step 3: Classification of Threats in distinct categories –Gates
- Step 4: Addressing Security Requirements based on identified threats and challenges
- Step 5: Determination of objectives in Cloud-based Health Systems
- Step 6: Determination of Assets in Cloud-based Health systems
- Step 7: Definition of security policy rules and procedures

According to the results of our previous research work, the most important threats present in Cloud Computing environments are presented in [9,10,11]. The threats related specifically to Cloud-based health information systems are also presented in [29][30][31] and [32]. The identified threats have been classified in the following distinct Categories:

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

In order to achieve an adequate level of protection in a SaaS Cloud-based Health system, a risk assessment study has been 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 [29]. In the following section we will assess if the proposed security policy covers the main GDPR requirements classes (presented in Table 1). In cases where the existing security policy [29] does not cover, or partially covers, the GDPR requirements, new policy rules are being proposed.

4. Results

4.1. Compliance with our Security Policy Methodology with GDPR

In this section, the security policy for Cloud-based health information systems proposed in [1], will be extended in order to cover the GDPR provisions of Table 1.

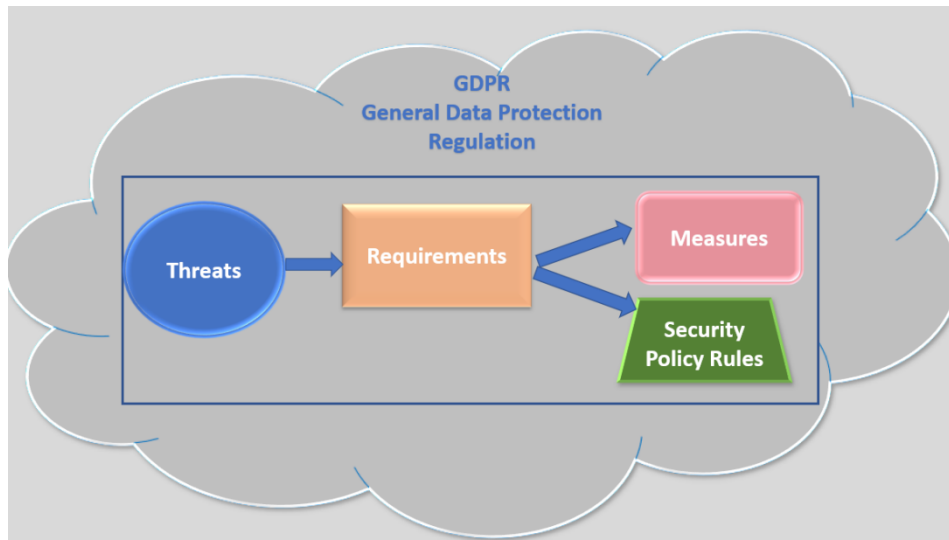


Figure 3 Overall Methodology of Cloud -based Security Policy compliant with the GDPR

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

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 [A]
Increased Territorial Scope	o	See [B]
Appoint a Data Protection Officer	-	See [C]
Breach Notification	-	See [D]
Privacy by design	●	See [1]
Data Protection Impact Assessment	-	See [E]
Penalties	-	See [F]
Consent/ Conditions for consent	-	See [G]
Independent Supervisory Authorities	-	See [H]
Data Protection by Design and default	o	See [1] [I]
Records of processing activities	●	See [1]
●: Covered -: Not Covered o: Partially Covered		

This table aims to generate value for the health-care 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 the patients' there are some steps health-care organizations should take to benchmark their current compliance, so 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

A. Rights of Data Subjects

In order for Cloud-based Health Organizations and Providers to be able to manage the requests of the Data Subjects who use their services, concerning the exercise of their rights, we propose a specific procedure that Cloud Health Organizations and Provider should follow:

- identify the details of the Data Subjects
- evaluate their requests
- decide whether to satisfy them or not, while also informing them

Step 1: Collection of Data Subject's Request

The communication channels that Cloud-based Health Organization supports and the Data Subjects can use in order to the exercise their rights are three:

- Physical Presence: The Data Subject completes a standardized form on the premises of Cloud-based Health Organization
- Website: The Data Subject, after visiting the website of Cloud-based Health Organization, completes the online form for exercising the rights of the Data Subjects
- Mail (physical or electronic): The Data Subject can exercise one of its rights by writing free text and sending it to Cloud-based Health 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 the reception of the request, the responsible department / responsible person who receives it must, within a reasonable time, proceed to identify the Data Subject who filed the request and to update the provided communication data in case 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, 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, Cloud-based Health Organization must manage the request and respond within thirty (30) days, with the possibility of extending additional sixty (60) days. In case that it is not possible to verify the identity of the Data Subject by Cloud-based Health Organization, according to the above table, then the Data Subject's request may be rejected. The process continues to Step 3

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

Cloud-based Health 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 the 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 Health Organization.
- The date the Data Subject was identified.
- The date of the response by Cloud-based Health 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 responsible department / person who received it, must be sent to the Data Protection Officer. Therefore, any department of Cloud-based Health Organization that receives a request regarding the rights of the subject have to forward it to the Data Protection Officer, so that his/her assessment is carried out and the 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, he/she assesses whether the information is sufficient or whether he/she needs additional information from the Data Subject in order to effectively assess the request.

If the available information is considered 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 his/her possession is sufficient, he/she is in a position to proceed with an effective assessment of the Data Subject 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 ought, among others, to seek the necessary information through the available information systems and / or to get in contact with the departments of Cloud-based Health Organization which may be related to the request of the Data Subject.

In addition, the Processing Activities Record, where all personal data processing activities for which Cloud-based Health 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 purpose of processing.
- The recipients of the data inside and outside of Cloud-based Health Organization.
- The legal basis of the processing
- 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 his rights and classify it as "Request can be settled", "Request can be settled but a charge is raised for the subject", or "Request cannot be settled".

In the following table an indicative guide concerning the assessment of the requests is presented:

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 a charge is raised for the subject	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 his 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 his data but has previously requested the erasure of the data.

If the request is assessed as "Request can be settled but a charge is raised for the subject", 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.

However, in any case, the Data Protection Officer informs the competent departments of the Cloud-based Health 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 competent department of 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 competent department of the Cloud-based Health 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

Cloud-based Health Organization must be able to satisfy the rights of the Data Subjects. Depending on the option(s) that Cloud-based Health Organization will define, the Data Protection Officer will be able to communicate with the Data Subject via printed or electronic media.

One Form for exercising Data Subject's Rights must be available both in printed form at Cloud-based Health Organization infrastructures and in 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 Health Organization for exercising their rights. In order to satisfy the right to information and access, Cloud-based Health Organization may use one document as a Response template. In order to satisfy the rights of rectification, erasure, objection, limitation of processing, data portability, Cloud-based Health Organization, in cooperation with the Data Protection Officer, should develop technical mechanisms to support these requests.

Cloud-based Health Organization should maintain a "Requests record" where details of how each data subject's request has been satisfied can be found.

Cloud-based Health Organization may communicate the responses to the requests of the Data Subjects by letter either in 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 competent department is responsible for informing the Data Subject in case that their request cannot be satisfied by Cloud-based Health Organization 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 will be satisfied promptly by Cloud-based Health 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 8**.

Step 10: Informing the DPO regarding the implementation

Once the competent department or departments 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 analyse all available information, whether the source is the Data Subject or deriving from the actions of the other competent departments of Cloud-based Health Organization, and to prepare the response to the Data Subject. These actions are carried out in any case; fulfilment of the request or not. In any case, the answer given to the

Data Subject regarding the fulfilment or not of the request must be documented. The procedure continues to **Step 12**.

Step 12: Informing the Data Subject regarding the fulfilment or not of the request

The competent department of the Cloud-based Health Organization must inform the Data Subject appropriately for the fulfilment or not of his/her request.

Therefore, the response to the Data Subject is communicated by the responsible department to the Data Subject via the selected communication channel. Indicatively:

- 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 competent 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 Health Organizations complies with the relevant GDPR requirements. The procedure is completed.

B. Increased Territorial Scope

In order to be able to manage the Increased Territorial Scope, Cloud-based Health 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 US).

PR4 - Activities 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- BCRs - Binding corporate rules as new appropriate safeguards should be taken.

C. Appoint a Data Protection Officer

Cloud-based Health Organizations and Providers should have a Data Protection Officer (DPO) and should adopt the following Security Policies:

PR1 - Review the current job specification of organization's DPO

PR2 - The DPO should report directly to the board, have independence, 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- Liability: The 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 processor must set appropriate technical and organizational measures to ensure an appropriate level of security

PR10 -The controller has the obligation to inform the Authority and the client as long as the breach poses a serious risk.

PR11- Codes of Ethics: 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.

D. Breach Notification

In order to be able to manage the Breach Notification, Cloud-based Health 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 preventing 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 patient when a data breach accident will happen

PR9 - Notify the national Authority within 72 hours in case of data breach.

E. Data Protection Impact Assessment

In order to be able to manage the Data Protection Impact Assessment, Cloud-based Health Organizations and Providers should adopt the following Security Policies:

PR1 - Keep and document all information of data processing, such as what personal data is collected, 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, with whom the data is being shared.

PR4 - keep a record of how long the data is to be stored.

PR5 - Ensure the data is encrypted, in order to protect them 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 e.g. through the use of CCTV or health monitoring devices.

PR9 - Adopt standards and show compliance through certification. In the case of Cloud-based health 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

F. Penalties

In order to be able to manage the Penalties, Cloud-based Health Organizations and Providers should adopt the following Security Policies:

PR1 - If the Health-care 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.

G. Consent/ Conditions for consent

In order to be able to manage the conditions for consent, Cloud-based Health 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 in case you rely on that for 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 individuals are aware of the process for withdrawing their consent

H. 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 will need are:

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.

I. Data Protection by Design and default

In order to be able to manage the Data Protection by Design and Default, Cloud-based Health Organizations and Providers should adopt the following Security Policies:

PR1 - Keep and document all information of data processing, such as what personal data is collected, how is 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, With whom the data is being shared.

PR4 – keep a record of how long the data is to be stored. And while being stored.

PR5- ensure the data is 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 Health hospitals, the components should be compliant to industry standards GDPR or to 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 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-minimising mechanisms

PR14- Appropriate privacy protection measures have to be implemented

PR15 - Update the procedures for dealing with requests and the satisfaction of citizens' rights, in particular as regards the deletion of data (right to forgiveness) 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 you collect and process.

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 Health information systems that satisfies the main requirements introduced by the General Data Protection Regulation. Furthermore it allows stakeholders working with Cloud-based health data to acquire more awareness in data protection rules that and allow EU citizens to have control over their personal data. The adoption of these security policy rules will enhance patients' trust since there is a secure Cloud environment that guarantees the patients' data are respected.

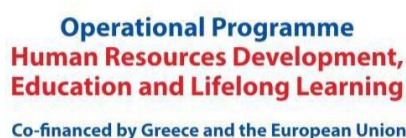
The policy issues presented in this paper are considered the basic pertaining to the GDPR in healthcare Cloud-based sector, but are not analytical and exhaustive. This research aim at providing practical advice and instruction to the EU Cloud-based Health institutions to comply with General Data Protection Regulation (GDPR), by helping them assess and manage the risks for data protection, privacy and other fundamental rights of individuals whose personal data are processed by cloud-based services. 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 cloud area.

Summarizing, this study identifies GDPR challenges that may emerge while adopting GDPR for private Cloud-based Health Systems. It presents 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 Health Framework of a national nature is a prerequisite. This Cloud Security Framework starts and ends with patient's need. They are the owners of their data and they should know what benefit they will have from the GDPR in a Cloud-based Health System and how much they will simplify their life and increase their degree of service.

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).



References

1. Georgiou Dimitra, PhD Thesis: Security Policies for Cloud Computing University of Piraeus,2018, http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/11007/Georgiou_Dimitra.pdf?sequence=1&isAllowed=y
2. 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. <https://eur-lex.europa.eu/eli/reg/2016/679/oj> Accessed 2 May 2017.

3. 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 <https://eur-lex.europa.eu/eli/dir/1995/46/oj>
4. Council of Europe Handbook on European data protection law 2018 edition https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf
5. Article 4 <https://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm>
6. Art. 9 GDPR Processing of special categories of personal data <https://gdpr-info.eu/art-9-gdpr/>
7. Convention 108 + Convention for the protection of individuals with regard to the processing of personal data <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>
8. Art.5 GDPR - Principles relating to processing of personal data <https://www.privacy-regulation.eu/en/>
9. Georgiou, D., & Lambrinouidakis, C. (2014). A Security Policy for Cloud Providers. In Proceedings of the 9th International Conference on Internet Monitoring and Protection (ICIMP 2014) (pp. 13-21).
10. Georgiou, D., & Lambrinouidakis, C. (2015, December). Cloud Computing Security Requirements and a Methodology for Their Auditing. In International Conference on e-Democracy (pp. 51-61). Springer, Cham.
11. Georgiou, D., & Lambrinouidakis, C. (2017). Security policy rules and required procedures for two crucial cloud computing threats. *International Journal of Electronic Governance*, 9(3-4), 385-403.
12. Art.5 GDPR - Principles relating to processing of personal data <https://www.privacy-regulation.eu/en/>
13. Article 12 EU GDPR -Transparent information, communication and modalities for the exercise of the rights of the data subject"<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>
14. Wooten, R., Klink, R., Sinek, F., Bai, Y., & Sharma, M. (2012), Design and Implementation of a secure Healthcare Social Cloud System. Proceedings of 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing.
15. 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 Journal*, 160-165, 2008
16. Zanaboni P, Wootton R. Adoption of telemedicine: from pilot stage to routine delivery. *BMC Med. Inform. Decis. Mak.* 2012;12:1.
17. Mehraeen, Esmail et al. "Security Challenges in Healthcare Cloud Computing: A Systematic Review." *Global journal of health science* 9 3 (2016): 59729.
18. A. Zriqat, "Security and Privacy Issues in Ehealthcare Systems : Towards Trusted Services," vol. 7, no. 9, pp. 229–236, 2016.
19. P. D. G. Vyawahare, R. B. Bende, D. N. Bhajipale, R. D. Bharsakle, and A. G. Salve, "A Survey on Security Challenges and Solutions in Cloud Computing," pp. 4069–4073, 2016.
20. Johnstone, M. (2012). Cloud security: A case study in telemedicine. 1st Australian e-Health Informatics and Security Conference, December 3rd-5th, Perth, Western Australia.
21. Cheng, F. C., & Lai, W. H. (2012). The Impact of Cloud Computing Technology on Legal Infrastructure within Internet—Focusing on the Protection of Information Privacy. *Procedia Engineering*, 29, 241-251. <http://dx.doi.org/10.1016/j.proeng.2011.12.701>
22. A. R. Alzoubaidi, "Cloud Computing National e-health services:Data Center Solution Architecture," *Int. J. Comput. Sci. Netw. Secur.*, vol. 16, no. 9, pp. 1–6, 2016.
23. M. Plachkinova, A. Alluhaidan, and S. Chatterjee, "Health Records on the Cloud : A Security Framework," pp. 152–158.
24. M. M. Noufal, "Smart e-Health Monitoring and Maintenance Using Cloud," no. 3, pp. 61–65, 2016.
25. A. A. V. Rani and E. Baburaj, "An efficient secure authentication on cloud based e-health care system in," pp. 53–59, 2016.
26. N. Dong, H. Jonker, and J. Pang, "Challenges in eHealth: from enabling to enforcing privacy," in *Foundations of Health Informatics Engineering and Systems. FHIES 2011. Lecture Notes in Computer Science*, Z. Liu and A. Wassylng, Eds., pp. 195–206, Springer, 2011.
27. Velumadhava, R. R., & Selvamani, K. (2015). Data Security Challenges and Its Solutions in Cloud Computing. *Procedia Computer Science*, 48, 204-209. <http://dx.doi.org/10.1016/j.procs.2015.04.171>
28. Balasubramaniam, S., & Kavitha, V. (2015). Hybrid Security Architecture for Personal Health Record Transactions in Cloud Computing. *Advances in Information Sciences and Service Sciences*, 7(1): 121-130.

29. Georgiou D., Lambrinouidakis C. (2020) Security and Privacy Issues for Intelligent Cloud-Based Health Systems. In: Maglogiannis I., Brahnam S., Jain L. (eds) Advanced Computational Intelligence in Healthcare-7. Studies in Computational Intelligence, vol 891. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-61114-2_9
30. Cloud Security Alliance (2018). Top Threats to Cloud Computing: Deep Dive 2018 <https://downloads.cloudsecurityalliance.org/assets/research/top-threats/top-threats-to-cloud-computing-deep-dive.pdf>, Accessed 30 September 2018
31. ENISA (2018). Threat Landscape Report 2018 15 Top Cyber threats and Trends <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018>, Accessed 25 November 2018
32. ISACA (2012) Security Considerations for Cloud Computing https://www.isaca.org/bookstore/Pages/Product-Detail.aspx?Product_code=SCC Accessed 25 November 2018