future internet

MDPI

Article

Data Protection Impact Assessment (DPIA) for Cloud-Based Health Organizations

Dimitra Georgiou * and Costas Lambrinoudakis

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

Abstract: The General Data Protection Regulation (GDPR) harmonizes personal data protection laws across the European Union, affecting all sectors including the healthcare industry. For processing operations that pose a high risk for data subjects, a Data Protection Impact Assessment (DPIA) is mandatory from May 2018. Taking into account the criticality of the process and the importance of its results, for the protection of the patients' health data, as well as the complexity involved and the lack of past experience in applying such methodologies in healthcare environments, this paper presents the main steps of a DPIA study and provides guidelines on how to carry them out effectively. To this respect, the Privacy Impact Assessment, Commission Nationale de l'Informatique et des Libertés (PIA-CNIL) methodology has been employed, which is also compliant with the privacy impact assessment tasks described in ISO/IEC 29134:2017. The work presented in this paper focuses on the first two steps of the DPIA methodology and more specifically on the identification of the *Purposes of Processing* and of the data categories involved in each of them, as well as on the evaluation of the organization's GDPR compliance level and of the gaps (*Gap Analysis*) that must be filled-in. The main contribution of this work is the identification of the main organizational and legal requirements that must be fulfilled by the health care organization. This research sets the legal grounds for data processing, according to the GDPR and is highly relevant to any processing of personal data, as it helps to structure the process, as well as be aware of data protection issues and the relevant legislation.

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

Citation: Georgiou, D.; Lambrinoudakis, C. Data Protection Impact Assessment (DPIA) for Cloud-Based Health Organizations. *Future Internet* **2021**, *13*, 66. https://doi.org/10.3390/fi13030066

Academic Editor: Joel J. P. C. Rodrigues

Received: 29 December 2020
Accepted: 3 March 2021
Published: 7 March 2021

1. Introduction

Digital cloud services are affecting the healthcare sector by injecting huge innovation, improving the quality of care, and strengthening the doctor-patient relationship. However, by their very nature, such services collect and manage a large amount of sensitive (health) data and thus need to comply with the security and privacy requirements raised by the General Data Protection Regulation (GDPR) [1]. The development of cloud services that process health data in accordance with legal requirements, may be risky, painful, and costly, due to the possibility of data loss and subsequent fines.

As privacy concerns spread through society and more specifically to the healthcare sector, the importance of the Data Protection Impact Assessment (DPIA) increases, especially since under GDPR, organizations must conduct a DPIA when a processing activity is likely to result "*in high-risk to the rights and freedoms of natural persons*" [2] (Article 35). Although GDPR does not precisely specify the types of processing activities for which a DPIA would be necessary, through the guidelines that it provides, it is clear that the organization should conduct a DPIA if there is large scale processing of health (sensitive) data. Hospital Information Systems (HISs) are typical examples of systems that store and process large amounts of sensitive data in order to offer a variety of medical services [3].

Furthermore, GDPR aims to protect data subjects concerning the processing of personal data. Recital 84 [4] says "*in order to enhance compliance with this Regulation where*

processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a Data Protection Impact Assessment (DPIA) to evaluate, in particular, the origin, nature, particularity, and severity of that risk".

Therefore, it is safe to say the DPIAs benefits are 2-fold: (a) To understand and mitigate risks to peoples' rights and (b) to satisfy the legal requirements [5].

The outcome of a properly conducted DPIA will be the minimization of privacy, security and reputation risks, compliance with the data protection legislation, and enhanced trust among data subjects and stakeholders.

DPIA is a concept in complete harmony with GDPR's philosophy, calling for the protection of data subjects from "*high risks*" through timely planning and obtaining all the necessary precautionary measures. The Data Controller and the Data Processor need to comply with the principle of accountability, or in other words be always able to prove that they have taken all the appropriate measures to protect the personal data and ensure compliance. The estimation of the impact forms a potential incident and helps fulfill both aspects of the accountability principle, since depending on the risk that may arise from the processing of data and on the weighting (impact) of this risk estimated during the DPIA, the appropriate protection measures will be identified.

The earlier we identify threats that pose a "risk" to personal data, the better the accuracy and effectiveness of the measures that will be adopted for the protection of the data. The process of early identification of potential risks and the integration of appropriate protection measures during design is known as "privacy by design".

However, the process of conducting a DPIA for a hospital can be complex and requires special skills. Although almost 3 years have passed since GDPR is in effect, organizations still face difficulties to comply. This is particularly challenging for healthcare organizations, due to the lack of resources and expertise. This paper presents the main steps of a DPIA study and provides guidelines on how to carry them out effectively. To this respect, the Privacy Impact Assessment, Commission Nationale de l'Informatique et des Libertés (PIA-CNIL) methodology has been employed, which is also compliant with the privacy impact assessment tasks described in ISO/IEC 29134:2017. The work presented in this paper focuses on the first two steps of the DPIA methodology and more specifically on the identification of the *Purposes of Processing* and of the data categories involved in each of them, as well as on the evaluation of the organization's GDPR compliance level and of the gaps (*Gap Analysis*) that must be filled-in. The main contribution of this work is the identification of the main organizational and legal requirements that must be fulfilled by the health care organization.

This paper acts as a precursor to a full DPIA for Health Information Systems, and applies to patients' personal data processed in all forms of media, including paper records, electronic records, images, videos, SMS texts, online postings, and electronic messages, as used in the provision of care.

The remaining sections of the paper are organized as follows: Section 2 describes the steps of the PIA-CNIL [6] methodology in brief. Section 3 employs a case study of a cloud-based Hospital Information System, in order to present the first two steps of the DPIA. More specifically, it analyzes the context of personal data processing in a hospital, the purposes of processing, the personal data required for the processing, and focuses on a Gap Analysis in terms of the issues that must be addressed in order to achieve compliance with the GDPR. Finally, Section 4 concludes the paper and presents issues for further research.

2. Description of the DPIA Steps

Clearly, the provision of cloud-based health services involves "high-risk" processing on a high volume of data and thus the DPIA is a necessary step in order to protect the privacy and the rights of the patients.

Based on the literature research we present, through a case study, the steps necessary for conducting a DPIA that will ensure the security and privacy aspects of a cloud-based Health Information System and more specifically the GDPR principles, such as purpose

limitation, data minimization, accuracy, accountability, the lawfulness of processing, and the user consent (Article 5) [7].

In this regard, the hospital information system will respect all the data owners' rights (patients), such as their rights to object to the storage/processing of their data, their right to be forgotten, and their right to the restriction of processing (Article 12–23) [8], while the obligations of the intermediate users, such as health professionals, production managers, and in general all the professional profiles that manage the system and potentially exploit all the data generated within the cloud-based system are specified. Finally, all the necessary technical, organizational, and procedural measures for the satisfaction of the eliciting security and privacy requirements are considered, thus enhancing confidence and trust among all stakeholders.

As already mentioned, the DPIA process is not strictly defined. The data controller can develop its own template or use a template provided by someone else. In our case study, we will employ the methodology proposed by the French Data Protection Authority (CNIL) [6]. Its main steps/stages, as well as the transition from one stage to the other, are depicted in Figure 1.

Figure 1. General approach of the privacy impact assessment, Commission Nationale de l'Informatique et des Libertés (PIA-CNIL) methodology.

More specifically, the four steps of the PIA-CNIL methodology are:

1. Define in detail the context of the processing of personal data under consideration. Provide a brief description of the project including its nature, scope, content, and purposes. Moreover, the data controller must identify the data processors, if any. In addition, the precise personal data that will be collected and processed must be defined together with their recipients, the duration of storage, and the processing activities from their collection to their deletion. This step also contains the identification of the personal data supporting assets for the under-examination system. Summarizing, this step aims to define the outline of the personal data processing process, such as the categories of the personal data, the purpose of processing, the way data are processed, the personal data supporting assets, the data subjects, etc.
2. Identify the existing and planned controls (procedural/technical/organizational) that are necessary for protecting the data, treating privacy risks in a proportionate manner, and achieving compliance with legal requirements. Justify and explain the choices made regarding the purpose for which the data are collected, their storage period, and their quality. More specifically, a clear description/documentation of the way that the following legal requirements are satisfied, is necessary: 1. Clear description of the purpose of personal data processing, 2. Data minimization (only the absolutely necessary data for serving the specific purpose of processing are collected), 3. Quality of data (data are correct and kept up-to-date), 4. Retention periods (for how long are the data stored), 5. Information (ensure that the data subjects are informed about the way their data are processed), 6. Ensure that the processing is performed legally, identifying the appropriate legal basis (for instance, the consent of the data subjects),

7. Right to object (respect the data subjects' right of opposition), 8. Right of access (respect the data subjects' right to access all the data stored for her), 9. Right to rectification, 10. Transfers (ensure compliance with obligations relating to the transfer of data outside the European Union). Finally, the existing controls are identified and classified in three categories: Organizational Procedural, Logical Security, and Physical Security controls.

3. Assess the privacy risks associated with the data processing and ensure they are properly treated. In this step, the Sources of Risks should be identified in the specific context under consideration as well as the Description of the capabilities of these sources of risks. In addition to this, in this step, the Feared events should be defined and more specifically, for each feared event (*illegitimate access to personal data, unwanted change of personal data, and disappearance of personal data*): The Determination of the potential impacts on the data subjects' privacy (*if it occurred*) and the Estimation of its severity, depending especially on the prejudicial effect of the potential impacts. Then, in this step, the Threats should be defined, and more specifically the Threats to personal data supporting assets that could lead to each feared event. Thus, for each identified threat the Selection of the risk sources that could cause it and the Estimation of its likelihood, particularly depending on (the level of vulnerabilities of personal data supporting assets, the level of capabilities of the risk sources to exploit them, and the controls likely to modify them) should be analyzed. Finally, in this step, the Risks should be identified and more specifically, the Determination of the risk level: Its severity equals that of the feared event concerned by the risk and its likelihood equals the highest likelihood value of the threats associated with the feared event.
4. The objective of this step (Risk management decisions) is the review of the results of the preceding steps, the evaluation of the risk level and the already existing controls, and the determination of whether or not they are acceptable. In case modifications are needed, an action plan is developed for the improvement of this state. In this step, the already existing controls are evaluated for the satisfaction of legal requirements and decisions are made on whether existing controls are satisfactory. When not, an action plan is prepared and validated.

3. Case Study: A Cloud-Based Hospital Information System

3.1. Context of Personal Data Processing

The first step of a DPIA is to determine the personal data processing context and thus, in this case, for the services provided by either a cloud-based Health Information System, operated by the hospital itself or by a data processor on behalf of the hospital. This system stores and displays health records for patients/healthcare service users and the medical professionals. It is clear that the system has a wide range of assets that are essential for the operation and thus need to be protected.

According to the PIA-CNIL methodology, in the analysis of the processing context, a particular emphasis is placed on the description of the data being processed and on the assets that support the data processing. The supporting assets include hardware, software applications, processing activities, organizational measures, and related roles. Additionally, when analyzing the processing context, the purpose of processing and any codes of conduct or other arrangements governing the processing of personal data are identified.

3.2. Description of Personal Data Processing in a Hospital

Based on the hospital's objectives and the replies received by the end users, there is processing of personal data and special categories of personal data for the following purposes of processing:

- PP1: Personnel Management
- PP2: Financial Management
- PP3: Business Development
- PP4: Provision of Patients Care-Services (Patients Monitoring Service)

Services related to the aforementioned purposes of processing include the following processing activities (Table 1).

Table 1. Identified data processing activities.

Purpose of Processing		Processing Activities
PP1	Personnel Management	HR management Health and Safety management
PP2	Financial Management	Payroll Co-funded Projects–Government Grants
PP3	Business development	Business development
PP4	Provision of Patients Care-Services	Hospital administration User management

3.3. Personal Data Required for the Data Processing

The following sections present the data processed for the processing activities for each of the above cases.

3.3.1. Personal Data for the Purpose of Processing PP1: Personnel Management

The data involved in the processing activities for Personnel Management is categorized into two groups based on their criticality:

- Personal data (Article 4 of GDPR [1]): This category contains the personal data of employees.
- Special categories of personal data (Article 9 of GDPR [1]): This category contains employees' health data (for instance, serious illnesses or handicaps) and work accidents.

Table 2 shows, for each data category, the data processed:

Table 2. Data processed under personnel management.

Personal Data	
Data Categories	**Indicative Data**
Personal data	Employees' personal data (name, surname, father's name, mother's name, SSN, Police ID card number, TIN, postal address, telephone, CVs and copies of diplomas, work related data)
Special Categories of Personal Data	
Data Categories	**Data**
Special categories of personal data	Employees' health data (serious illnesses or handicaps etc.), work accidents

3.3.2. Personal Data for the Purpose of Processing PP2: Financial Management

The data involved in the processing activities for Financial Management is again divided in two categories, as shown in Table 3:

Table 3. Data processed under financial management.

Personal Data	
Data Categories	Indicative Data
Personal data	Accountants' personal data (name, surname) Employees' personal data (name, surname, father's name, mother's name, SSN, Police ID card number, postal address, telephone, salary, work hours, project work related data)
Special Categories of Personal Data	
Data Categories	Data
Special categories of personal data	Employees' health data for illness leaves

3.3.3. Personal Data for the Purpose of Processing PP3: Business Development

The data involved in the processing activities for Business Development are only personal data, as shown in Table 4.

Table 4. Data processed under business development.

Personal Data	
Data Categories	Indicative Data
Personal data	Business contacts' personal data (name, surname, gender, postal address, telephone, e-mail, age group, education level) Business contacts' profiling data: Personality-Attitude towards hospital, Hierarchy level, Job title/responsibilities, Department/medical unit of work, Therapy addressed/knowhow, Accessed route addressed/practice, Infusion method/practice/choice, Number of patients treated/managed per year

3.3.4. Personal Data for the Purpose of Processing PP4: Provision of Patients Care-Services

The data involved in the processing activities for the Provision of Patients Care-Services is divided in two categories, as shown in Table 5:

Table 5. Data processed in patients care-services.

Personal Data	
Data Categories	Data
Personal data	Patients' personal data (First name, Last name, Date of birth—age, Gender, Phone number, Email address, Login email, Mobile phone) Healthcare professionals' personal data (First name, Last name, Specialty, Phone number, Email address, Login email, Mobile phone) Patient portal users' personal data (First name, Last name, Phone number, Email address, Login email, Mobile phone, Relation to patient) Sales staff/Distributors' sales staff (First name, Last name, Phone number, Email address, Login email, Mobile phone) Activity Log of access/actions of users related to a patient therapy Users (i.e., Healthcare professionals, staff, personal data (First name, Last name, Phone number, Email address, Login email, Mobile phone)
Special Categories of Personal Data	
Data Categories	Data
Special categories of personal data	Patients' health data: Treatments (pain management, chemotherapies) Treatment information: Start date, Prescriptions, Administered medications, Infusion data (e.g., volume delivered, pump alarms), Clinical observations (e.g., pain level)

3.4. Existing and Planned Controls (Procedural/Technical/Organizational)

Having identified the Purposes of Processing and the data involved in each processing activity, it is necessary to decide if a DPIA is necessary on not. According to the GDPR *Article 35* [5]: " . . . *Where a type of processing in particular using new technologies, and taking*

into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data . . . . . A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale.". Taking into account the criticality of the data processed by the hospital for the "Provision of Patients Care-Services (PP4)" purpose of processing, it is necessary to perform a privacy impact assessment study, as the hospital carries out the processing of special categories of personal data on a large-scale (guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (4 October 2017)), which could be characterized as a high risk processing.

This is not the case for the remaining purposes of processing.

Thus, for PP4 it is necessary to proceed with the second step of the DPIA methodology in order to identify the existing and planned controls (procedural/technical/organizational) that are necessary for protecting the data, treating privacy risks in a proportionate manner, and achieve compliance with legal requirements.

To do that, a Gap Analysis, in relation to the requirements of the General Data Protection Regulation 2016/679 (GDPR), for the specific purpose of processing was performed. The results of this Gap Analysis (presented in Table 6) raise the organizational and legal requirements that must be satisfied by the hospital.

Table 6. Findings of the gap analysis for the processing activity, PP4: Provision of Patients Care-Services in relation to the requirements of the general data protection regulation.

Regulation's Article [ ]	Article's Subject	Compliance Activities/Demands	Activities Status	Compliance
Article 5	"Principles relating to processing of personal data (a) lawfulness, fairness, and transparency (b) purpose limitation (c) data minimization (d) accuracy (e) storage limitation (f) integrity and confidentiality"	Conduct a DPIA (a) lawfulness, fairness, and transparency (b) purpose limitation (c) data minimization (f) integrity and confidentiality	IN PROGRESS	NO
		Data Protection Policy Process to maintain data quality (d) accuracy	NOT IMPLEMENTED	
		Data Protection Policy Process for data retention period (e) storage limitation	NOT IMPLEMENTED	
		Maintain records of processing activities	IN PROGRESS	
		Maintain documents as a proof of compliance	NOT IMPLEMENTED	
Article 6	Lawfulness of processing	Conduct a DPIA Lawfulness of processing	IN PROGRESS	
		Maintain documents to prove the lawfulness of processing (Law, contracts, consent forms, etc.)	NOT IMPLEMENTED	
		Data Protection Policy *Process for acquiring data subjects' consent*	NOT IMPLEMENTED	
		Data Protection Policy *Process for secondary use of personal data*	NOT APPLICABLE	
Article 7	Conditions for consent	Data Protection Policy Process for acquiring data subjects' consent	NOT IMPLEMENTED	NO
		Data Protection Policy Process for managing/satisfying the rights of the data subjects	NOT IMPLEMENTED	
Article 8	Conditions applicable to child's consent in relation to information society services	Data Protection Policy Process for acquiring child's consent through the approval of the child's parental responsibility	NOT APPLICABLE	YES

Table 6. *Cont.*

Regulation's Article [ ]	Article's Subject	Compliance Activities/Demands	Activities Status	Compliance
Article 9	Processing special categories of personal data	Conduct a DPIA Lawfulness of processing special categories of personal data	IN PROGRESS	NO
		Maintain documents to prove the lawfulness of processing special categories of personal data (Law, contracts, consent forms, etc.)	NOT IMPLEMENTED	
		Data Protection Policy Process for acquiring and using data (including special categories of personal data)	NOT IMPLEMENTED	
Article 10	Processing personal data relating to criminal convictions and offences	Conduct a DPIA Lawfulness of processing	NOT APPLICABLE	YES
		Maintain documents (Law, contracts, consent forms etc.) to prove the lawfulness of processing personal data relating to criminal convictions and offences	NOT APPLICABLE	
		Data Protection Policy Process for acquiring and using data (including personal data relating to criminal convictions and offences)	NOT APPLICABLE	
Article 12	Transparent information, communication, and modalities for the exercise of the rights of the data subject	Data Protection Policy Process for informing data subjects about the ways of processing their data	NOT IMPLEMENTED	NO
		Data Protection Policy Process for managing/satisfying the rights of the data subjects	NOT IMPLEMENTED	
		Data Protection Policy Process for notifying the supervisory authority/data subjects about a personal data breach	NOT IMPLEMENTED	
Article 13	t Information to be provided where personal data are collected from the data subject	Data Protection Policy Process for informing data subjects about the ways of processing their data	NOT IMPLEMENTED	
		Data Protection Policy Process for managing/satisfying the rights of the data subjects	NOT IMPLEMENTED	
		Data Protection Policy Process for acquiring and using data	NOT IMPLEMENTED	
		Data Protection Policy Process for secondary use of personal data	NOT APPLICABLE	
		Data Protection Policy Process for notifying the supervisory authority/data subjects about a personal data breach	NOT IMPLEMENTED	
Article 14	Information to be provided where personal data have not been obtained from the data subject	Data Protection Policy Process for informing data subjects about the ways of processing their data	NOT APPLICABLE	
		Data Protection Policy Process for managing/satisfying the rights of the data subjects	NOT APPLICABLE	
		Data Protection Policy Process for acquiring and using data	NOT APPLICABLE	
		Data Protection Policy Process for secondary use of personal data	NOT APPLICABLE	
		Data Protection Policy Process for notifying the supervisory authority/data subjects about a personal data breach	NOT APPLICABLE	
Article 15	Right of access by the data subject	Data Protection Policy Process for managing/satisfying the rights of the data subjects	NOT IMPLEMENTED	NO
Article 16	Right to rectification	Data Protection Policy Process for managing/satisfying the rights of the data subjects	NOT IMPLEMENTED	NO
Article 17	Right to erasure ("right to be forgotten")	Data Protection Policy Process for managing/satisfying the rights of the data subjects	NOT IMPLEMENTED	NO
Article 18	Right to restriction of processing	Data Protection Policy Process for managing/satisfying the rights of the data subjects	NOT IMPLEMENTED	NO
Article 19	Notification obligation regarding rectification or erasure of personal data or restriction of processing	Data Protection Policy Process for management/satisfaction of the rights of the data subjects (including process of informing the subjects of changes made by the organization)	NOT IMPLEMENTED	NO
Article 20	Right to data portability	Data Protection Policy Process for managing/satisfying the rights of the data subjects	NOT APPLICABLE	YES
Article 21	Right to object	Data Protection Policy Process for managing/satisfying the rights of the data subjects	NOT IMPLEMENTED	NO

Table 6. *Cont.*

Regulation's Article [ ]	Article's Subject	Compliance Activities/Demands	Activities Status	Compliance
Article 22	Automated individual decision-making, including profiling	Data Protection Policy Process for managing/satisfying the rights of the data subjects	NOT IMPLEMENTED	NO
Article 24	Responsibility of the controller	Conduct a DPIA (if required)	IN PROGRESS	NO
		Data Protection Policy	NOT IMPLEMENTED	
		Data Protection Policy Process for determining the obligations of processors (if any)	NOT APPLICABLE	
		Data Protection Policy Process for internal review/auditing of policy implementation	NOT IMPLEMENTED	
		Maintain documents as a proof of compliance	NOT IMPLEMENTED	
Article 25	Data protection by design and by default	Conduct a DPIA (if required)	IN PROGRESS	NO
		Data Protection Policy Process for accommodating data protection by design and by default specifications	NOT IMPLEMENTED	
Article 26	Joint controllers	As for Data Controller (Articles 24 and 25)	NOT APPLICABLE	YES
		Maintain documents to define the obligations as to the lawfulness of data processing and satisfaction of the rights of the data subjects	NOT APPLICABLE	
Article 27	Representatives of controllers or processors not established in the Union	Data Protection Policy Process for immediate notification of the controller and the data subjects (if necessary) about a personal data breach	NOT IMPLEMENTED	NO
Article 28	Processor	Data Protection Policy Process for checking the compliance of the processors with the obligations set by the controller	NOT APPLICABLE	YES
		Data Protection Policy Process for immediate notification of the controller and the data subjects (if necessary) about a personal data breach	NOT APPLICABLE	
Article 29	Processing under the authority of the controller or processor	Data Protection Policy Process for checking the compliance of those involved (subcontractors) with the data processing with the terms that the controller or the processor has included in their contracts	NOT APPLICABLE	YES
Article 30	Records of processing activities	Maintain records of processing activities	IN PROGRESS	NO
Article 32	Security of processing	Conduct a risk analysis study	IN PROGRESS	NO
		Security measures based on the risk level (e.g., pseudonymization, encryption, access control, firewall, network intrusion detection, logs, etc.)	IN PROGRESS	
		Data Protection Policy Process for Aligning Data Protection Policy with Security Policy	NOT IMPLEMENTED	
Article 33	Notification of a personal data breach to the supervisory authority	Data Protection Policy Process for notifying the supervisory authority/data subjects about a personal data breach	NOT IMPLEMENTED	NO
		Maintain a record of incidents/breaches	NOT IMPLEMENTED	
		Maintain the list of notifications to the supervisory authority/data subjects about a personal data breach	NOT IMPLEMENTED	
		Maintain a record/log of actions when dealing with a data breach	NOT IMPLEMENTED	
Article 34	Communication of a personal data breach to the data subject	Data Protection Policy Process for notifying the supervisory authority/data subjects about a personal data breach	NOT IMPLEMENTED	NO
		Maintain a record of incidents/breaches	NOT IMPLEMENTED	
		Maintain the list of notifications to the supervisory authority/data subjects about a personal data breach	NOT IMPLEMENTED	
		Maintain a record/log of actions when dealing with a data breach	NOT IMPLEMENTED	
Article 35	Data protection impact assessment	Conduct a DPIA (if required)	IN PROGRESS	NO
Article 36	Prior consultation	Consultation of PIAs results with the Supervisory Authority (if required)	NOT APPLICABLE	YES
Article 37	Designation of the data protection officer	Designation of the Data Protection Officer (DPO) (if required)	IMPLEMENTED	YES
Article 38	Position of the data protection officer	Independence, regular communication/collaboration, accountability of DPO with the management	IMPLEMENTED	YES
		Confirmation of non-conflict of interest of the DPO with other duties and obligations of the organization	IMPLEMENTED	

Table 6. *Cont.*

Regulation's Article [ ]	Article's Subject	Compliance Activities/Demands	Activities Status	Compliance
Article 39	Tasks of the data protection officer	Is the DPO designated (if required) with her duties set?	IMPLEMENTED	YES
Article 44	General principle for transfers	Maintain Documentation to Confirm the lawfulness of Personal Data transfers to Third Countries or International Organizations (e.g., Law, Consent forms, Public Interest, Standard Contractual Clauses, Binding Company Rules, Regulatory Approvals, etc.) Depending on the legal basis, check the required evidence in Articles 45 to 49.	NOT APPLICABLE	YES
Article 45	Transfers on the basis of an adequacy decision	Control of data transfer mechanism	NOT APPLICABLE	YES
Article 46	Transfers subject to appropriate safeguards	Control of data transfer mechanism	NOT APPLICABLE	YES
Article 47	Binding corporate rules	Control of data transfer mechanism (Binding Corporate Rules (BCRs))	NOT APPLICABLE	YES
Article 48	Transfers or disclosures not authorised by Union law	Control of data transfer mechanism	NOT APPLICABLE	YES
Article 49	Derogations for specific situations	Control of data transfer mechanism	NOT APPLICABLE	YES
Article 89	Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes	Data Protection Policy Procedure for data anonymization for processing related to scientific research/statistical research	NOT IMPLEMENTED	NO
		Keeping documentation for deviations from the GDPR due to special processing cases (if required)	NOT APPLICABLE	
Article 91	Existing data protection rules of churches and religious associations	Data Protection Policy	NOT APPLICABLE	YES

From the gap analysis findings, the following set of organizational/legal requirements in Table 7 has been derived, aiming to the satisfaction of all the "In progress" and "Not Implemented" cases in Table 6.

Table 7. General data protection regulation (GDPR) requirements derived from the gap analysis.

Organizational/Legal Requirements	
Requirement ID	**Requirement**
GDPR-01	Conduct a Data Protection Impact Assessment regarding the processing of personal data
GDPR-02	Conduct a Data Protection Impact Assessment regarding the lawfulness of processing
GDPR-03	Conduct a Data Protection Impact Assessment regarding the Lawfulness of processing of special categories of personal data
GDPR-04	Conduct a Data Protection Impact Assessment regarding the Responsibility of the controller
GDPR-05	Conduct a Data Protection Impact Assessment regarding the Data protection by design and by default principle
GDPR-06	Conduct a Data Protection Impact Assessment regarding the security of processing
GDPR-07	Conduct a Data Protection Impact Assessment as demanded by Article 35 of the GDPR regulation
GDPR-08	Define a Data Protection Policy for describing the process to maintain data quality
GDPR-09	Define a Data Protection Policy for describing the process for data retention period
GDPR-10	Define a Data Protection Policy for describing the process for acquiring data subjects' consent
GDPR-11	Define a Data Protection Policy for describing the process for managing/satisfying the rights of the data subjects
GDPR-12	Define a Data Protection Policy for describing the process for acquiring and using data (including special categories of personal data)
GDPR-13	Define a Data Protection Policy for describing the process for informing data subjects about the ways of processing their data
GDPR-14	Define a Data Protection Policy for describing the process for notifying the supervisory authority/data subjects about a personal data breach
GDPR-15	Define a Data Protection Policy for describing the process for internal review/auditing of policy implementation
GDPR-16	Define a Data Protection Policy for describing the process for accommodating data protection by design and by default specifications
GDPR-17	Define a Data Protection Policy for describing the process for immediate notification of the controller and the data subjects (if necessary) about a personal data breach
GDPR-18	Define a Data Protection Policy for describing the process for Aligning Data Protection Policy with Security Policy

Table 7. *Cont.*

Organizational/Legal Requirements	
Requirement ID	**Requirement**
GDPR-19	Define a Data Protection Policy for describing the process for data anonymization for processing related to scientific research/statistical research
GDPR-20	Maintain records of processing activities
GDPR-21	Maintain documents as a proof of compliance
GDPR-22	Maintain documents to prove the lawfulness of processing
GDPR-23	Maintain documents to prove the lawfulness of processing of special categories of personal data
GDPR-24	Maintain a record of incidents/breaches
GDPR-25	Maintain the list of notifications to the supervisory authority/data subjects about a personal data breach
GDPR-26	Maintain a record/log of actions when dealing with a data breach
GDPR-27	Conduct a Risk Analysis Study
GDPR-28	Define security measures based on the risk level (e.g., pseudonymization, encryption, access control, firewall, network intrusion detection, logs, etc.)

Thus, the aforementioned organizational and legal requirements must be satisfied by the hospital. In addition, to those, it is necessary to perform a risk analysis in order to identify potential threats and existing vulnerabilities together with an estimation of the impact that a security incident may cause to the stakeholders of the system (hospital/patients), and thus to elicit the security and privacy requirements that should also be addressed by the hospital in order to protect the data and the privacy of the patients.

3.5. Remaining DPIA Steps

Having completed the first two steps of the DPIA methodology, we can proceed with the assessment of the privacy risks associated with the data processing and ensure they are properly treated (Step 3), as well as with the validation of the way it is planned to comply with privacy principles and treat the risks (Step 4). The aforementioned steps are not addressed in this paper.

4. Conclusions

The global dimension of cloud computing requires standardized methodologies and technical solutions in order to enable stakeholders to assess privacy risks and establish adequate protection levels. The cloud presents new challenges for compliance and many cloud services are not GDPR ready. For this reason, the Data Protection Impact Assessment study is a useful tool, aiming to assess the privacy risks involved in processing operations. A DPIA is the basis of a "privacy by design" approach and helps organizations meet the privacy and data protection expectations of their customers, employees, and other stakeholders.

Although conducting a DPIA is now a legal requirement under the GDPR [1], it is not mandatory for all processing operations, but only for those involving high risks to the rights and freedoms of their subjects. Data controllers should consider conducting a Data Protection Impact Assessment in such processing operations, as a useful and positive activity that helps them demonstrate compliance with the law. Currently, there is a lack of methodology offering systematic support for the process of DPIA in cloud-based Health Information Systems. Our work seeks to fill this gap by providing the appropriate guidelines.

In this paper, we have presented the first two steps of a DPIA for a cloud-based Health Information System, based on the PIA-CNIL methodology [6]. Through the case study employed, we have identified the *Purposes of Processing* and the data categories involved in each of them. Furthermore, we have demonstrated how to evaluate the organization's GDPR compliance level through a *Gap Analysis*. Finally, the main organizational and legal requirements that must be fulfilled by the health care organization, were identified.

As GDPR touches on all aspects of a hospital and more specifically on a cloud-based Health Information System, we are currently working on a framework to enable the non-stressful implementation of a DPIA. In our future work, we will focus on the remaining DPIA steps, providing the appropriate guidelines for their effective implementation.

Author Contributions: Conceptualization, D.G. and C.L.; methodology, D.G. and C.L.; validation, D.G. and C.L.; investigation, D.G. and C.L.; resources, D.G. and C.L.; writing—original draft preparation, D.G.; writing—review and editing, D.G. and C.L.; supervision, 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 (IKY).

Data Availability Statement: Not Applicable, the study does not report any data.

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. Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 12 September 2020).
2. ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Data Protection Impact Assessment (DPIA) and Determining whether Processing Is "Likely to Result in A High Risk" for the Purposes of Regulation 2016/679. Available online: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (accessed on 1 August 2020).
3. Shabani, M.; Borry, P. Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. *Eur. J. Hum. Genet.* **2018**, *26*, 149–156. [CrossRef] [PubMed]
4. Recital 84 EU GDPR. Available online: https://www.privacy-regulation.eu/en/recital-84-GDPR.htm (accessed on 11 September 2020).
5. Article 35 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices and Agencies and on the Free Movement of Such Data, and Repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725 (accessed on 15 October 2020).
6. French Data Protection Authority Privacy Impact Assessment (PIA). Available online: https://www.cnil.fr/en/privacy-impact-assessment-pia (accessed on 3 March 2021).
7. Art. 5 GDPR Principles Relating to Processing of Personal Data. Available online: https://gdpr-info.eu/art-5-gdpr/ (accessed on 16 December 2020).
8. Art. 12–23 Rights of the Data Subject 7. Available online: https://gdpr-info.eu/art-5-gdpr/ (accessed on 20 December 2020).