DPIA for Cloud-based Health Organizations in the Context of GDPR

Dimitra Georgiou and Costas Lambrinoudakis
Department of Digital Systems, University of Piraeus, Piraeus, Greece

dimitrageorgiou@ssl-unipi.gr
clam@unipi.gr

Abstract: The General Data Protection Regulation is the core instrument of the reformed legal framework for personal data protection in the European Union. The GDPR was put into effect on May 25, 2018, and requires assessing and conducting a Data Protection Impact Assessment for processing operations that are likely to result in a high risk to the rights and freedoms of natural persons, specifically using new technologies and considering the nature, scope, context, and purposes of the processing. Although GDPR does not precisely specify the types of processing activities for which a DPIA would be necessary, through the guidelines that it provides, the organization should conduct a DPIA, if there is large scale processing of health data. An example of this, is a Cloud-based Health Organization. Taking into account this parameter, that Cloud-based Health Organization processes personal data that could impact the freedoms and rights of a data subject under the GDPR and that the GDPR does not specify a DPIA process to follow, instead it allows organizations to use a framework that complements their existing processes, this paper presents the last two steps of a DPIA study for a Cloud-based Health Organization and provides guidelines on how to carry them out effectively. This study is part of a project for the compliance of Cloud-based Health Organizations with the General Data Protection Regulation 2016/679. For fulfilling the objectives of this study, the PIA-CNIL methodology is applied, which is in accordance with the data privacy impact assessment that has been described in ISO/IEC 29134. The main contribution of this work is the development of a guide that is designed to help Cloud-based Health organizations identify, analyze and reduce data protection risks in relation to their processing activities. More analytically, this research presents the risks that could be materialized by the data processing activities carried out by a Cloud-based Health Organization regarding its Processing Activities and could have an impact on the fundamental rights and freedoms of natural persons.

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

1. Introduction

The General Data Protection Regulation (European Union, 2016) is the most significant piece of privacy legislation to come into effect across Europe, affecting all sectors including healthcare. It is a common set of guidelines to control and to protect personal data and it brings significant changes to how organizations should manage and process personal data, the privacy risk assessments they conduct, and the privacy compliance programs they develop to mitigate the identified risks to the privacy of the data subjects. The GDPR applies to organizations located within the EU, as well as to organizations that offer services or monitor the behavior of EU residents regardless of the organization's location. Organizations serving every sector must respect the personal data they process, demonstrating compliance with the corresponding Regulation. The healthcare sector is among the most affected, for several reasons, including the problem of defining and dealing with the concept of personal data protection**.** And what does it mean? GDPR requires health organizations to take adequate measures to ensure the security of personal than with other types of data and a DPIA is mandatory for them. A DPIA is a risk technique mandated by the GDPR to enable organisations to address privacy concerns and ensure appropriate technical and organisational safeguards are addressed and built into new amendments of existing systems (David Wright, 2012). Under GDPR and Article 35, a DPIA is only mandatory where processing "...*is likely to result in a high risk to the rights and freedoms of natural persons*" (European Union, 2016). This includes automated decision-making, large-scale processing of special categories of data and systematic large-scale monitoring of public areas. As in the Cloud healthcarere domain all patients' data are considered "sensitive", it involves a large-scale processing volume of personal data and individuals are vulnerable. These characteristics meet three of the criteria described in (Chryssanthou et all, 2012) and therefore in the healthcare domain, data processing must be considered as possibly high-risk by default, thus implying that DPIA cannot be avoided. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR (David Wright, 2011) Despite the recent attempts to provide tools to assist institutions to comply with the GDPR and as Article 35 (European Union, 2016) does not provide an explicit description for the DPIA and specifically for cloud-based healthcare systems (Kush Wadhwa & Rowena Rodrigues, 2013) (Makri Eleni-Laskarina et al, 2019).

To summarize, this paper apart from the introduction is organized as follows. Section 2 provides a description of DPIA steps of PIA-CNIL Methodology, Section 3 provides information for the Case Study of Cloud-Based Hospital, Section 4 presents the Privacy Impact Assessment related to the processing activities of 'Patients Monitoring Service' implemented by Hospital as Data Processor, Section 5 presents the Risk management

decision related to the processing activities of Patients Monitoring Service. Finally, Section 6 concludes the paper by outlining aspects for further research.

2. Description of DPIA steps of PIA-CNIL Methodology

For the analysis and the privacy impact assessment of personal data, the (French Data Protection Authority, 2018) has proposed PIA-CNIL methodology. Performed in principle by a data controller, the purpose of a PIA is to build and demonstrate the implementation of privacy protection principles so that data subjects retain control over their personal data. It is intended for data controllers who wish to demonstrate their compliance approach, as well as for product and service providers wishing to show that their solutions do not breach privacy thanks to a design that respects privacy satisfaction of Article 25 (European Union, 2016). More specifically, to carry out a PIA it is necessary to (Dimitra Georgiou and Costas Lambrinoudakis, 2021):

1. Define and describe the context of the processing of personal data under consideration and its stakes.
2. Identify existing or planned controls (procedural / technical / organisational) guaranteeing compliance with legal requirements and to treat privacy risks in a proportionate manner.
3. Assess privacy risks associated with data security and ensure they are properly treated.
4. Make the decision to validate the way it is planned to comply with privacy principles and treat the risks or review the preceding steps.

The following **Error! Reference source not found.** depicts the main steps of PIA-CNIL methodology (French Data Protection Authority, 2018) and mentions the step 3 and step 4 that will be analysed in this paper. Furthermore, the objectives of all the steps of PIA- CNIL methodology are presented in the following paragraphs.

Figure 1: Steps of PIA-CNIL methodology (French Data Protection Authority, 2018)

The **first step – Context of personal data processing** aims at the definition of the outline of the processing of personal data, such as the categories of the processed personal data, their ways of processing, the purpose of processing, the personal data supporting assets, the data subjects, etc. This step contains the definition of the valuable for the under-examination system Assets:

- The description of the purpose of processing(s) of personal data.
- The identification of Data Controller and any Data Processor(s).
- The identification of the categories of personal data and their recipients.
- The identification of the retention period of personal data.
- The description of the processes and personal data supporting assets for the entire personal data life cycle (from collection to erasure).

The objective of the **second step – Controls** is to build a system that ensures compliance with privacy protection principles. This step requires compliance (and thorough documentation of the way to achieve it) with the following legal requirements (obligatory):

- Purpose of personal data processing: Specified, explicit and legitimate purpose.
- Data Minimisation: limiting the amount of personal data to what is strictly necessary.
- Quality of data: preserving the quality of personal data, accurate and kept up-to-date.
- Retention periods: period needed to achieve the purposes, in the absence of another legal obligation imposing a longer retention period.
- Information: respect for data subjects' right to information.
- Consent: obtaining the consent of the data subjects or existence of another legal basis justifying the processing of personal data.
- Right to object: respect for the data subjects' right of opposition.
- Right of access: respect for the data subjects' right to access their data.
- Right to rectification: respect for the data subjects' right to correct their data and erase them.
- Transfers: compliance with obligations relating to transfer of data outside the European Union

Moreover, the existing controls are identified or determined:

- Organisational controls: organisation policy, risk management, project management, incident management, supervision, etc.
- Logical security controls: anonymisation, encryption, backups, data partitioning, logical access control, etc.
- Physical security controls: physical access control, security of hardware, protection against non-human risk sources, etc.

The objective of the **third step** Risks (Potential privacy breaches) of PIA-CNIL is to gain a good understanding of the causes of risks, the threats against privacy, as well as the impact of their potential realisation. In this step, the following should be defined:

- Sources of Risks
    - Identification of the relevant risk sources in the specific context under consideration
    - Description of the capabilities of risk sources
- Feared events
    - For each feared event (illegitimate access to personal data, unwanted change of personal data, and disappearance of personal data):
    - Determination of the potential impacts on the data subjects' privacy if it occurred.
    - Estimation of its severity, depending especially on the prejudicial effect of the potential impacts
- Threats
    - Identification of threats to personal data supporting assets that could lead to each feared event.
    - For each identified threat:
        - Selection of the risk sources that could cause it.
        - 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.
- Risks
    - Determination of the risk level:
        - Its severity equals to that of the feared event concerned by the risk.
        - Its likelihood equals the highest likelihood value of the threats associated with the feared event.

The objective of the **fourth 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 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 whether existing controls are satisfactory. When not, an action plan is prepared and validated.

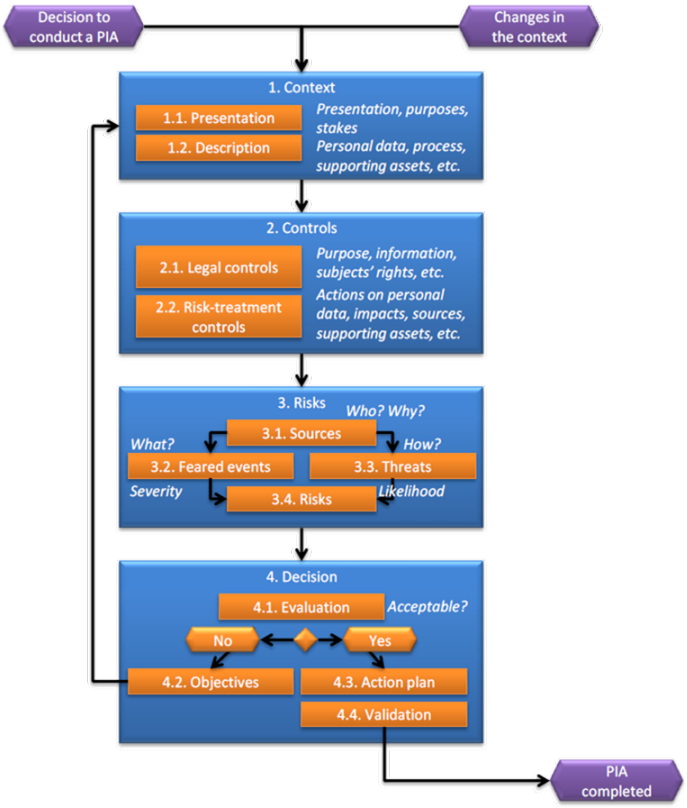

Figure 2: Detailed approach for carrying out PIA-CNIL Methodology (French Data Protection Authority, 2018)

3. Case Study: A Cloud-Based Hospital -Theoretical Background

This document primarily refers to the case study of a Cloud-based Hospital, however its results are applicable to all entities as far as organisational and operational issues are concerned. Furthermore, different Organisations can use the approach used in this case study as guidance of the information that needs to be included in a DPIA, making adaptations where necessary depending on the circumstances of the case. Information regarding the on-premises ICT infrastructure is only applicable to this case study. In this regard, we indicate the steps of guidelines in designing and testing a DPIA process that is generic enough to be used in all possible application areas, but also able to consider the specifics of each area. For fulfilling the objectives of this study, PIA-CNIL methodology (French Data Protection Authority, 2018) is applied. This paper presents the Steps 3 and 4 of the DPIA Methodology, risks that could be materialised by the data processing activities carried out by Hospital regarding its Processing Activities and could have an impact on the fundamental rights and freedoms of natural persons. These Processing Activities will be implemented directly by Hospital as Data Processor. The risks for the fundamental rights and freedoms of natural persons that will be assessed in the context of the impact assessment in this paper are related with *illegitimate access to data, unwanted modification of data and data disappearance*. Since the analysis that has been conducted in paper (Dimitra Georgiou and Costas Lambrinoudakis, 2021) has revealed that this specific processing activity PP4: Patients Monitoring Service involves special categories of personal data on a large scale which could be characterised as a high risk processing and a Gap Analysis in relation to the GDPR requirements for this processing activity has been conducted, 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 even though this is an obligation of the Data Controller and not of the Hospital.

Impact assessment aims at the protection of personal data, as well as the protection of elements that support their processing and are recognised as Assets. The value of such assets is equal to the Impact brought upon by a possible violation of individuals' privacy. A Feared Event is the illegitimate access to personal data, unwanted modification of personal data, as well as the data disappearance. The violation of information systems needs the existence of Vulnerability and the appearance of a relevant Threat coming from a Risk source. Summarising, we note that a Threat exploits a vulnerability of an Information System and can have as a result an incident of data protection breach, inflicting some Impact on data subjects (**Figure** 33). The risk level is estimated in terms

of severity, which represents the magnitude of a risk. It essentially depends on the prejudicial effect of the potential impacts, and likelihood, which represents the possibility for a risk to occur. It essentially depends on the level of vulnerabilities of the supporting assets facing threats and the level of capabilities of the risk sources to exploit them (**Figure 3**).

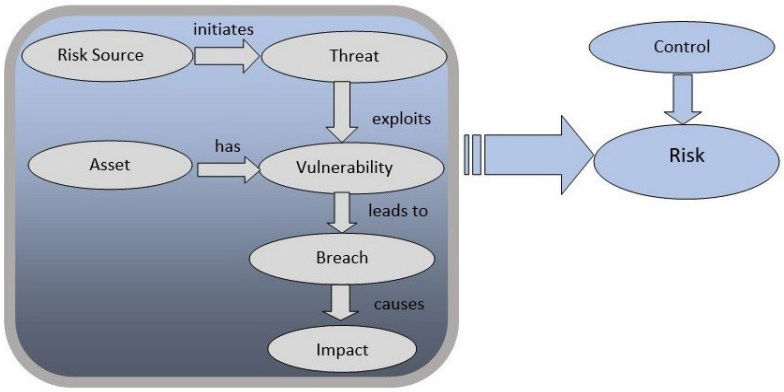

Figure 3: Conceptual Framework of Impact Assessment

4. Assessment of Privacy Risks related to the processing of "Patients Monitoring Service" (PP4)

4.1 Introduction

The following paragraphs describe the impact assessment for the potential violation of the privacy of the Cloud hospital's personal data (Georgiou and Lambrinoudakis, 2021) involved in the processing activities for the purpose of "*Patients Monitoring Service (PP4)".* This section analyses the personal data processed by hospital and the level of risk by determining the severity of the risk, which is the same as the severity of the data breach incident (feared event) that can be caused by the specific risk and by the likelihood. According to the PIA-CNIL methodology (French Data Protection Authority, 2018) feared events may have three different impacts if they occur (**Table** 1) causing data breaches. The severity of risk and the likelihood of a risk occurring are scaled in levels as presented later.

Table 2 contains the scales and rules for estimating severity, in terms of the extent of potential impacts on data subjects. Section 4.2 describes the processing activities related with platform and the purpose of Patients Monitoring Service, implemented by Hospital as Data Processor. All three categories of risks are analysed, as it is estimated that they can be materialised by the corresponding processing activities (Georgiou and Lambrinoudakis, 2021).

Table 1: Typology of the outcomes of feared events (French Data Protection Authority, 2018)

Feared events	Types of outcomes	Description
Illegitimate access to data	None	The data are seen by people who do not need to know them, though these people do not use them.
	Storage	The data are copied and saved to another location without being further used.
	Redistribution	The data are disseminated more than necessary and beyond the control of the data subjects.
	Use	The data are used for purposes other than those planned and/or in an unfair manner or correlated with other information relating to the data subjects.
Unwanted modification of data	Malfunction	The data are modified into valid or invalid data, which will not be used correctly, the processing liable to cause errors, malfunctions, or no longer provide the expected service.
	Use	The data are modified in other valid data, such that the processing operations have been or could be misused.
Disappearance of data	Malfunction	The data are missing for personal data processing, which generates errors, malfunctions, or provides a different service than the one expected
	Blockage	The data are missing for personal data processing which can no longer provide the expected service

Table 2: Scales and rules for estimating severity (French Data Protection Authority, 2018)

Levels	Generic description of impacts
Negligible	Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem.
Limited	Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties.
Significant	Data subjects may encounter significant consequences, which they should be able to overcome albeit with real and serious difficulties.
Maximum	Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome.

The aforementioned scale can be used to estimate the likelihood of threats (French Data Protection Authority, 2018):

1. Negligible: It does not seem possible for the selected risk sources to materialise the threat by exploiting the properties of supporting assets.
2. Limited: It seems difficult for the selected risk sources to materialise the threat
3. Significant: It seems possible for the selected risk sources to materialise the threat
4. Maximum: It seems extremely easy for the selected risk sources to materialise the threat.

4.2 Privacy Impact Assessment related to the processing activities of "Patients Monitoring Service"

Based on the requirements of the GDPR (Georgiou and Lambrinoudakis, 2020)and taking into account the criticality of the data processed by Hospital for the *Patients Monitoring* that Hospital implements as Data Processor (Georgiou and Lambrinoudakis, 2021)**,** we consider that it is necessary to perform a PIA study, as Hospital carries out processing of special categories of personal data on a large scale, which could be characterised as a high risk processing, according to the provisions of the Article 35 of GDPR (European Union, 2016).

The Hospital care platform is used to enable data processing for the purpose of Patients Monitoring. Hospital conducts processing of personal data and special categories of data that are hosted at the databases of the Hospital care platform. More specifically, Hospital supports through the platform staff or patients by managing therapies for both inpatients and outpatients. Hospital infusion devices communicate with Hospital care platform and transmit device data, which are stored and presented under the treatment context. The risks for the fundamental rights and freedoms of natural persons that are assessed in the context of the impact assessment are related with *illegitimate access to data, unwanted modification of data and data disappearance.*

4.2.1 Risk category: Illegitimate access to data

The risk of unauthorised access to data that Hospital care platform maintains can appear in the processing activities for patients monitoring due to various threats (Figure 3). This section discusses these threats grouped according to their nature or to the asset that they target and include masquerading of identity, unauthorised use of an application, threats during data transmission and misuse of physical resources of Hospital. The analysis of the impact of each threat is carried out in accordance with Typology of the outcomes of feared events (Table 1) and considers the potential for unauthorised storage, redistribution, or use of personal and sensitive data. Next, the components of risk per threat are analysed in the following parts:

Threat: Masquerading of User Identity
• **Masquerading of User Identity by Insiders** – The threat covers attempts by authorised users to gain access to information to which they have not been granted access. • **Masquerading of User Identity by Contracted Service Providers –** The threat covers attempts by people working for a contracted service provider to obtain unauthorised access to information by using an authorised person. • **Masquerading of User Identity by Outsiders** – The threat covers attempts by outsiders to obtain unauthorised access to information by posing as an authorised user.

Figure 4: Threat Masquerading of User Identity

Impact: Inappropriate use of patients' personal data, due to masquerading of users may result in the use of

sensitive data of platform for purposes other than the purpose originally set. *Severity*: Severity from threats of masquerading vary depending on the occurrence of the threat, but in its maximum appearance it leads to a maximum impact and is valued at level 4. *Likelihood:* Hospital implements some technical controls specific to protecting the digital identity of Hospital care users. Additionally, there has been no similar occurrence in the past, but incidents of stolen credentials are common. Based on this, it is estimated that the probability of the threat is negligible and is valued at level 1. *Risk sources:* employees of Hospital, former Hospital employees, external attackers, and any other Hospital care user, Malicious code of unknown origin. *Controls:* For the estimation of the impact, the implemented by Hospital controls have been considered.

Threat: Unauthorised Use of an Application
This Threat covers attempts of use of resources of technical aspects, in a non-compatible way to the provided authorisations and rights.

Figure 5: Threat Unauthorized Use of an Application

Impact: Incorrect use of data due to unauthorised use of an application may prevent the Hospital's provision of Hospital care services while the data may be used for purposes other than the purpose originally set. *Severity:* The severity of unauthorised access leads to a maximum impact and is valued at level 4. *Likelihood:* Hospital, imposed by hospital's security policy, takes high technical and organisational controls to prevent unauthorised access, such as strong password policy, multifactor authentication, https. Additionally, there has been no similar occurrence in the past. Based on this, it is estimated that the probability of the threat is limited and is valued at level 1. *Risk sources:* employees and former hospital employees, malicious code of unknown origin. *Controls:* For the estimation of the impact, the implemented by Hospital controls have been considered.

Threat: Threats during data transmission
• **Communication Interception** – This threat covers: passive interception and traffic monitoring. • **Accidental Mis-routing** – The threat covers the possibility that information might be delivered to an incorrect address.

Figure 6: Threat during the data transmission

*Impact***:** Attacks aimed at interfering with electronic communications, traffic monitoring or accidental misrouting can lead to leakage of patients' data. *Severity***:** Data transmission threats may lead to a significant impact and is valued at level 3. *Likelihood:* Hospital implements technical and organisational controls to prevent unauthorised access, such as https. Additionally, there has been no similar occurrence in the past. Based on this, it is estimated that the probability of the threat is negligible and is valued at level 1. *Risk sources:* employees and agents of Hospital who have access to the platform, former employees, external attackers, or any other user, malicious code of unknown origin. *Controls:* For the estimation of the impact, the implemented by hospital controls have been considered.

Threat: Misuse of physical resources
• **Theft (by Insiders)** – This threat would include anybody who had a legitimate reason to be working in the building. • **Theft (by Outsiders)** –Theft of any resources, as physical assets. It relates to thefts by outsiders. • **Terrorism** – Covers acts by extremist groups wishing to cause damage to the work of the organisation, or harm people

Figure 7: Threat Misuse of physical resources

Impact: Unauthorised access to data due to misuse of resources may prevent the hospital's provision of services and lead to significant impacts for both hospital and for the patients. *Severity:* Severity from misuse of physical resources threats leads to a significant impact and is valued at level 3. *Likelihood:* From hospital's point of view, the workspace is well monitored and there is access control system. Combining this with the absence of a past incident, it is estimated that the probability of the threat is negligible and valued at level 1. *Risk sources:* employees of hospital, former employees, and any other user, who had access to platform. *Controls:* For the estimation of the impact, the implemented by hospital controls have been considered. The list of implemented controls, will be presented in our new paper.

4.2.2 Risk category: Unwanted modification of data

The risk of unintended modification to Hospital data can be realised in the processing activities based upon various threats (Figure 3). This section addresses these threats grouped according to their nature or according to the asset they exploit, including masquerade, damage to hardware, and damage to software. The components of risk per threat are analysed in next paragraphs:

Threat: Masquerading of User Identity
• **Masquerading of User Identity by Insiders** – The threat covers attempts by authorised users to gain access to information to which they have not been granted access. • **Masquerading of User Identity by Contracted Service Providers –** The threat covers attempts by people working for a contracted service provider to obtain unauthorised access to information by using an authorised person. • **Masquerading of User Identity by Outsiders** – The threat covers attempts by outsiders to obtain unauthorised access to information by posing as an authorised user.

Figure 8: Threat Masquerading of user Identity

Impact: The masquerading of a user's identity can lead to unwanted modification of patients' data. This action can lead to a maximum impact on patients as the modification of information, can cause harm to the patient that may even lead to death. *Severity:* Based on the above, severity from threats vary depending on the occurrence of the threat, but in its maximum appearance it leads to a maximum impact and is valued at level 4. *Likelihood:* Hospital implements specific technical controls to protect the digital identity of Hospital care users. Additionally, there has been no similar occurrence in the past, but incidents of stolen credentials are common. Based on this, it is estimated that the probability of the threat is negligible and is valued at level 1. *Risk sources:* employees of Hospital, former Hospital employees, external attackers, malicious code of unknown origin. *Controls:* For the estimation of the impact, the implemented by Hospital controls have been considered.

Threat: Hardware Malfunction
Operations Error – The threat covers the possibility that the people responsible for operating the Host system might make mistakes when carrying out their work. **Hardware Maintenance Error** –The threat covers the possibility that those people responsible for maintaining the hardware might make mistakes when carrying out their work. **Staff Shortage** –The threat covers the possibility of the absence of key personnel for whatever reason and the ease with which they could be replaced.

Figure 9: Threat Hardware Malfunction

Impact: Insufficient hardware maintenance or operating mistakes on the hosting platform of hospital, may lead to availability or integrity loss of provided services. *Severity***:** severity from threats vary depending on the occurrence of the threat, but in its maximum appearance it leads to limited impact and is valued at level 2. *Likelihood:* Given to the contractual obligations and SLAs available, the possibility of hardware maintenance/operations errors, or insufficient support, is low. Based on this, it is estimated that the probability of the threat is valued at level 1. *Risk sources***:** Employees of hospital, incorrectly configured legal binding documents. *Controls:* For the estimation of the impact, it has been considered that hospital exhibits several security certifications and thus it has been assumed that the appropriate controls are in place.

Threat: Software Malfunction
• **Unauthorised Use of an Application** – The threat covers attempts of use of resources of technical aspects, in a non-compatible way to the provided authorisations and rights. • **Introduction of Damaging or Disruptive Software** – The threat covers: any forms of malicious software. • **Embedding of Malicious Code** – The threat covers: e-mail viruses, hostile mobile code. • **Software Maintenance Error** – The threat covers the possibility that those people or organisations responsible for maintaining software might make mistakes when carrying out their work.

Figure 10: Threat Software Malfunction

Impact: Damage to the software may result in modification of patients' data. This action can lead to a limited impact on data subjects as it can cause consequences for them. *Severity***:** Severity from software malfunction threats leads to a limited impact and is valued at level 2. *Likelihood:* Hospital takes appropriate technical and organisational controls to protect its software. Additionally, there has been no similar occurrence in the past. Based on this, it is estimated that the probability of the threat is negligible and is valued at level 1. *Risk sources:* employees who are responsible for handling Hospital systems and have access to the platform, external

attackers, malicious code of unknown origin. *Controls:* For the estimation of the impact, the implemented by Hospital controls have been considered.

4.2.3 Risk category: Data disappearance

This section discusses these threats grouped according to their nature or according to the asset that they exploit and includes masquerading, technical failure, application software failure, communication breaches, malfunction to physical resources of Hospital. The analysis of the impact of each threat is conducted according to **Error! Reference source not found.**(**Table** 1) and takes into account the possible malfunctioning processing and error causing through the processing of data or the possible loss of personal and sensitive data when they can no longer provide the expected service to data subjects. Next, the components of risk per threat are analysed.

Threat: Masquerading of User Identity
• **Masquerading of User Identity by Insiders** – The threat covers attempts by authorised users to gain access to information to which they have not been granted access. • **Masquerading of User Identity by Contracted Service Providers –** The threat covers attempts by people working for a contracted service provider to obtain unauthorised access to information by using an authorised person. • **Masquerading of User Identity by Outsiders** – The threat covers attempts by outsiders to obtain unauthorised access to information by posing as an authorised user.

Figure 11: Threat Masquerading of User Identity

Impact: The masquerading of any users' platform identity from internal or external attackers can lead to the deletion of the data. This action can lead to maximum impact on patient, as the unavailability of certain data, that may render a doctor incapable of providing appropriate treatment. *Severity:* Severity from threats vary depending on the occurrence of the threat, but in its maximum appearance it leads to a maximum impact and is valued at level 4. *Likelihood:* Hospital takes some specific technical controls to protect the digital identity of users. Additionally, there has been no similar occurrence in the past, but incidents of stolen credentials are common. Based on this, the probability of the threat is negligible and is valued at level 1. *Risk sources:* Malicious code of unknown origin. *Controls:* For the estimation of the impact, the implemented by Hospital controls have been considered.

Threat: Technical Failure
• **Technical Failure of Host** – This threat covers failures of the CPU or other hardware items. • **Technical Failure of Storage Facility** – This threat covers disk crashes and disk failures. • **Technical Failure of Network Distribution Component** – This threat covers failure of the network distribution component, • **Technical Failure of Network Gateway** – This threat covers failure of servers or network operation. • **Air Conditioning Failure** – The threat covers the possibility that work may have to be suspended because temperatures in the location fall outside of acceptable parameters.

Figure 12: Threat: Technical Failure

Impact: Possible technical failure of network components, can lead to loss of availability of provided services. This action can lead to a significant impact on patients as the integrity of their data is at stake. *Severity:* severity from threats of technical failure vary depending on the occurrence of the threat, but in its maximum appearance it leads to a significant impact and is valued at level 3. *Likelihood:* Hospital offers redundant components and thus availability of the provided service of the users may be lost. Based on this, it is estimated that the probability of the threat is limited and is valued at level 2. *Risk sources:* hospital's relevant hardware components in infrastructure. *Controls:* For the estimation of the impact, it has been considered that hospital exhibits several security certifications and thus it has been assumed that the appropriate controls are in place.

Threat: Application Software Failure
• **System and Network Software Failure** – The threat covers the possibility that the system or network software might fail. • **Application Software Failure** – The threat covers the possibility of errors being contained in application programs.

Figure 13: Threat Application Software

Impact: Software failure, can lead to the deletion of personal and sensitive data hosted on it. Appearance of the above threat is expected to have a limited impact on data subjects as, since appropriate controls, like back-up are available. *Severity:* Based on the above, severity from threats vary depending on the occurrence of the threat, but in its maximum appearance it leads to a negligible impact and is valued at level 1. *Likelihood:* It is estimated that the realisation of the threat is random, its probability is small, so it is valued at level 1. *Risk sources:* Application programming errors and bugs. *Controls:* For the estimation of the impact, the implemented by Hospital controls have been considered.

Threat: Communication breaches
• **Communication Infiltration** – The threat covers Hacking into a system, masquerading as a server, masquerading as an existing user of an e-commerce application, masquerading as a new user of an e-commerce application, denial of service, flaming attacks, spamming. • **Communication Manipulation** – The threat covers active interception, insertion of false messages, deliberate delivery out of sequence, deliberate delay of delivery, deliberate misrouting, if an attacker can force a message to be sent via a hostile host, the attacker may be in a position to intercept, alter and the forward the message. • **Communication Failure** – This threat covers: Unavailability of Service Provider, failure of data link, non-delivery of message, accidental delivery out of sequence, accidental delay in delivery, accidental denial of service.

Figure 14: Threat Communication Breaches

Impact: This category of threats includes attacks aimed at editing, inserting, or deleting data. *Severity:* The threat severity from threats to communications differs depending on the occurrence of the threat but in its maximum appearance it leads to a significant impact and is valued by a level 3. *Likelihood:* The hospital takes technical and organisational controls to protect communications and its network, such as firewall and https. In addition, no attacker has been documented with an important incentive to carry out such an attack. Based on this, it is estimated that the probability of the threat is limited and valued at level 2. *Risk sources:* former Hospital employees who had access to platform, malicious code of unknown origin. *Controls:* For the estimation of the impact, the implemented by Hospital controls have been considered.

Threat: Malfunction to physical resources
• **Power failure** – The threat covers the possibility that the power supply to the building may fail. • **Fire** – The threat covers the possibility of fire affecting any of the physical assets that make up a system. • **Water Damage** – The threat covers the possibility of water affecting any of the physical assets that make up a system. • **Natural disaster** – The threat of natural disaster covers the possibility of either a natural event, or manmade (such as traffic accidents), causing physical damage to the location or surrounding area. • **Wilful damage – vandalism (by Insiders)** – The threat covers acts of vandalism and other cases where physical damage is caused to IT systems or their supporting environment by people who have been granted access to the building. • **Wilful damage – vandalism (by Outsiders)** – The threat covers acts of vandalism and other cases where physical damage is caused to IT systems or their supporting environment by people who have not been granted access to the building. • **Terrorism** –The threat covers acts by extremist groups wishing to cause damage or disruption to the work of the organisation, or harm people working for the organisation. Types of terrorist attack include letter bombs and car bombs.

Figure 15: Threat Malfunction to physical resources

Impact: Possible failure can lead to loss of availability of provided services. *Severity:* severity from the above threats vary depending on the occurrence of the threat, but in its maximum appearance it leads to a significant impact and is valued at level 3. *Likelihood:* Hospital takes particularly technical and organisational controls to protect from malfunction to physical resources. Based on this, it is estimated that the probability of the threat is limited and is valued at level 1. *Risk sources:* Employees of hospital, Former employee's terrorist organisations, fire, flood, power failure. *Controls:* For the estimation of the impact, hospital exhibits security certifications and thus it has been assumed that the appropriate controls are in place.

4.2.6 Overview of risks

The overall results of the risk assessment per risk category are outlined in the following Figures:

Risk category: Illegitimate access to data		
Threat	**Severity**	**Likelihood**
➢ Masquerading of User Identity	Maximum, Level: 4	Negligible, Level: 1
➢ Unauthorised Use of an Application	Maximum, Level: 4	Negligible, Level: 1
➢ Threats during data transmission	Significant, Level: 3	Negligible, Level: 1
➢ Misuse of physical resources	Significant, Level: 3	Negligible, Level: 1
MEAN ASSESSMENT VALUE	**3,5≈4 Maximum Level: 4**	**1 Negligible Level: 1**
GRAPHIC ANALYSIS		
Severity	(Undefined) Negligible Limited Significant	
Likelihood	(Undefined) Negligible Limited Significant	

Figure 16: Results of the Risk assessment for the illegitimate access to data

Risk category: Unwanted modification of data		
Threat	**Severity**	**Likelihood**
➢ Masquerading	Maximum, Level: 4	Negligible, Level: 1
➢ Hardware Malfunction	Significant, Level: 2,5≈3	Negligible, Level: 1
➢ Software Malfunction	Limited, Level: 2	Negligible, Level: 1
MEAN ASSESSMENT VALUE	**2,8≈3 Significant Level: 3**	**1 Negligible Level: 1**
GRAPHIC ANALYSIS		
Severity	(Undefined) Negligible Limited Significant Maximum	
Likelihood	(Undefined) Negligible Limited Significant Maximum	

Figure 17: Results of the Risk assessment for the Unwanted modification of data

Risk category: Data disappearance		
Threat	**Severity**	**Likelihood**
➢ Masquerading	Maximum, Level: 4	Negligible, Level: 1
➢ Technical failure	Significant, Level:3	Limited, Level:2
➢ Application Software Failure	Limited, Level: 2	Negligible, Level: 1
➢ Communications breaches	Significant, Level: 3	Limited, Level: 2
➢ Malfunction to physical resources	Significant, Level:3	Negligible, Level: 1
MEAN ASSESSMENT VALUE	**3 Significant Level: 3**	**1,3≈1 Negligible Level: 1**
GRAPHIC ANALYSIS		
Severity	(Undefined) Negligible Limited Significant Maximum	
Likelihood	(Undefined) Negligible Limited Significant Maximum	

Figure 18: Results of the Risk assessment for the Data disappearance

5. Risk management decision related to the activities of Patients Monitoring Service

The objective of the Step 4 is the review of the results of the preceding steps, the evaluation of the risk level and the already existing controls and the determination whether 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 whether existing controls are satisfactory. When not, an action plan is prepared and validated. A Risk mapping enables graphical identification of the risk, which in turn enables the carrier to identify parts of the infrastructure and its functions, which require corrective actions to address the risks arising for the protection of rights and freedoms of data subjects. Based on the identification of the risks in this situation, targeted corrective actions are chosen seeking to reduce the

impact of a risk or the likelihood of a threat. The corrective actions as well as the intended risk minimisation that follows the implementation of these actions will be presented in a new paper.

6. Conclusions and Further Research

Compliance with GDPR requirements is a challenge for the entire health community, as technological advances expand the frontiers of areas such as Cloud Computing storage. Complex and large-scale data processing activities in the health sector require careful planning and execution. An important tool to ensure that all relevant stakeholders in an organization assess GDPR requirements is the DPIA. In this paper we described a methodology specific for the Cloud-based Health Information Systems able to support the risk assessment and to perform a DPIA. The main contribution of this work is the development of a guide that is designed to help Cloud-based Health Organizations identify the information system threats (cclassification of threats) per risk category and reduce data protection risks in relation to their processing activities. The methodology was successfully applied in a real environment The risks examined in this paper are related with illegitimate access to data, unwanted modification of data and data disappearance. For the processing activities of Patients Monitoring Service, implemented by Hospital as Data Processor, the threats that may lead to the aforementioned risks and have the maximum likelihood to occur were: Masquerading of User Identity, Misuse of physical resources, Technical failure, Communication breaches, Malfunction to physical resources. From the aforementioned threats, the ones with the maximum severity to the rights and freedoms of natural persons were: Masquerading of User Identity (maximum severity), Misuse of physical resources (significant severity), Communication breaches (significant severity). The risk illegitimate access to data is assessed with a maximum level of severity and limited likelihood of occurring. The risks unwanted modification of data and data disappearance are assessed with a significant level of severity and limited likelihood of occurring. As the factors determining the risk level are the severity of the impact and likelihood of occurring. In a next paper, we will present the controls that will be chosen to be applied so as to demonstrate compliance with the GDPR and to offer the appropriate level of protection.

References

Chryssanthou et all, 2012. Hospital Information Systems Replacement and Healthcare Quality. *International Journal of Reliable and Quality E-Healthcare (IJRQEH),* 1(3), p. 12.

David Wright, 2011. Should privacy impact assessments be mandatory?. *Communications of the ACM,* August, 54(8), p. 121–131.

David Wright, P. H., 2012. Privacy Impact Assesment. In: P. H. David Wright, ed. *Law, Governance and Technology Series.* Dordrecht: Springer, pp. 3-32.

European Union, 2016. REGULATION (EU) 2016/679 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 Reg. *Official Journal of the European Union.*

French Data Protection Authority, 2018. *Commission Nationale de l'Informatique et des Libertés.* [Online] Available at: https://www.cnil.fr/en/privacy-impact-assessment-pia [Accessed 1 09 2022].

Georgiou and Lambrinoudakis, 2020. Compatibility of a Security Policy for a Cloud-Based Healthcare System with the EU General Data Protection Regulation (GDPR). *Information,* 11(12)(586), p. 19.

Georgiou and Lambrinoudakis, 2021. Data Protection Impact Assessment (DPIA) for Cloud-Based Health Organizations. *Future Internet,* 7 March, 13(3)(66), p. 12.

Kush Wadhwa & Rowena Rodrigues, 2013. Evaluating privacy impact assessments, 26:1-2,. *Innovation: The European Journal of Social Science Research,,* 21 March, 26(1-2), pp. 161-180.

Makri Eleni-Laskarina, G. Z. L. C., 2019. A proposed privacy impact assessment method using metrics based on organizational characteristics. In: *Computer Security: ESORICS 2019 International Workshops, CyberICPS, SECPRE, SPOSE, and ADIoT.* Luxembourg: s.n., pp. 122-139.