Informatics in Medicine Unlocked 19 (2020) 100361

Contents lists available at ScienceDirect

Informatics in Medicine Unlocked

journal homepage: http://www.elsevier.com/locate/imu

# Methodology and workflow to perform the Data Protection Impact Assessment in healthcare information systems

Marco Todde [a], Marco Beltrame [b], Sara Marceglia [a,*], Cinzia Spagno [b]

[a] Dipartimento di Ingegneria e Architettura, Università degli Studi di Trieste, Trieste, Italy
[b] Azienda Sanitaria Universitaria Giuliano Isontina - ASUGI, Trieste, Italy

ARTICLE INFO

*Keywords:*
General regulation on data protection
Hospital information system
Data protection impact assessment

ABSTRACT

*Background:* The General Regulation on Data Protection (GDPR) modernizes and harmonizes personal data protection laws across the European Union, affecting all economic sectors including the healthcare industry. The new regulation introduces two specific duties: the Record of Processing Activities (ROPA) and, for each high-risk processing, the Data Protection Impact Assessment (DPIA). Currently, there are no specific DPIA methodologies for the healthcare environment, but only broad methodologies applicable in all economic sectors.
*Objectives:* This work aims to propose a methodology to perform DPIA for healthcare information systems, considering the specific constraints and criticisms posed by the heterogenous and highly sensitive nature of data and software use in hospitals.
*Methods:* We first performed a GDPR analysis and an examination of other sources regarding DPIA. This analysis led to the identification of issues related to GDPR application in the healthcare environment. We then developed a workflow for DPIA execution, and implemented a software to apply it in a real environment. The methodology was applied on 11 softwares and devices already in use in the Trieste area, Italy.
*Results:* The most important issue identified in the analysis is the definition of "processing activity", which was overcome by focusing the methodology on the information system processing the data instead of the processing activity *per se*. We therefore designed a workflow for the risk assessment of an information system establishing that the DPIA shall be performed after the purchase, usually a bid with strict IT security requirements of the information system, but before its deployment in the real environment. The validation of the developed software to implement the workflow on the 11 softwares showed the ability of the proposed workflow to perform the DPIA, and to uncover some important issues in the examined systems.
*Conclusions:* The proposed methodology can be applied to perform DPIA in the healthcare environment by supporting risk evaluation and management, focusing on each software component added to the healthcare information system.

## 1. Introduction

The European Union (EU) General Data Protection Regulation (GDPR) [1] was issued in May 2018 and was directly applied in all EU member states. It was then extended in July 2018 to the European Economic Area (EEA) [2] thus affecting a larger number of countries. The implications of the GDPR have however consequences worldwide and in all economic sectors, being that data management is the core of present economies. Healthcare practice and research are among the most affected areas, for several reasons, including the management of healthcare data for secondary research use [3–6], as well as the impact on hospital information systems which are in the need to comply to GDPR rules, according to the concept of "accountability" [7,8].

Despite the recent attempts to provide software tools to allow research institutions to comply with the GDPR accountability requirement [7], there are still unsolved issues, especially for Hospital Information Systems (HISs) utilized in clinical practice, and not only in research.

The GDPR introduces two specific duties, namely the Record of Processing Activities (ROPA) and, for each high-risk processing, the Data Protection Impact Assessment (DPIA), that HISs should also perform. These are both described within the regulation and its

* Corresponding author. Dipartimento di Ingegneria e Architettura, Università degli Studi di Trieste, Via Valerio 10, 34127, Trieste, Italy.
*E-mail address:* smarceglia@units.it (S. Marceglia).

https://doi.org/10.1016/j.imu.2020.100361
Received 16 March 2020; Received in revised form 13 May 2020; Accepted 30 May 2020
Available online 31 May 2020

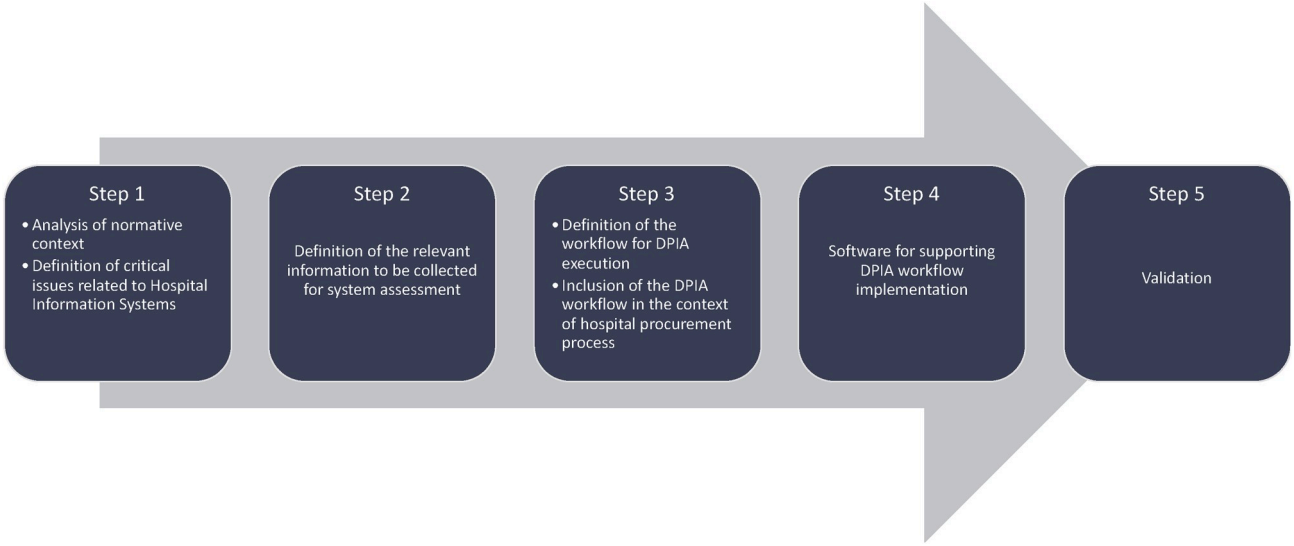


**Fig. 1.** Methodology development steps.

guidelines, but their practical application remains debatable.

The ROPA includes a minimum dataset of information (as specified in GDPR, art 30) that defines each processing made by the controller or the processor, which are the two entities involved in the protection of personal data. Then, if a processing poses high risks to the rights and the freedom of individuals, a DPIA shall be performed, as stated in the GDPR, art 35. The DPIA shall contain a description of the nature, scope, context, and purpose of the processing, its risk evaluation and assessment, compliance measures, and additional mitigation risks measures.

The definition of "high risk" processing is provided by the guidelines on the impact of data protection [9], which define nine criteria to assess whether a specific processing is likely to result in high risks to individuals. If a processing satisfies at least two out of nine criteria, this should be included in a DPIA. In the healthcare domain, all data are considered "sensitive" by definition; it involves a large volume of personal data (large-scale processing), and individuals are vulnerable. These three characteristics meet three of the criteria described in Ref. [9], and, therefore, in the healthcare domain, data processing must be considered as possibly high-risk by default, thus implying that DPIA cannot be avoided.

Hospital Information Systems (HISs) are usually characterized by several software applications, used to support a wide range of services, and several medical devices, running medical software applications, which are installed or substituted nearly every year [9]. It is self-evident that nearly every application in the healthcare enterprise and within the HIS is in the scope of DPIA, because, at least in part, each is used to treat a huge amount of sensitive data.

Moreover, there are some specific issues in managing the assessment of such applications/equipment. The practical chance of performing an effective DPIA is strictly connected to contractual bindings and e-procurement outcomes, because usually hospitals and healthcare facilities do not address software development, and, therefore, cannot control the implementation of privacy by design [10]. The procurement process of the healthcare sector should follow specific rules of transparency, and the medical equipment market is not yet ready to fulfill all the basic requirements of the latest information security guidelines (e.g. compliance with CIS critical security Controls, provisioning of NEMA MDS2 form, etc.). In the literature there are some papers facing DPIA in procurement processes, but none is focused on practical public e-procurement for clinical practice.

Those issues cause the application of GDPR in HISs, and in particular the DPIA, to be complex due to the need of selecting methods and solutions which have to be sustainable in terms of resources consumed (people and time) and compatible with current regulations.

Despite the introduction of the GDPR, which dates back one year, there are no specific methodologies for DPIA in healthcare, and, more specifically, in HISs.

As an example of the need for supporting tools in DPIA, Dashti and colleagues [11] proposed a tool to assist controllers to facilitate data subject's rights and freedoms, which is however not focused to the healthcare specific environment.

In this work, we aim to propose a methodology that is grounded on regulations, standards, and applicable norms, but considers the constraints and criticisms of the HIS environment, and allows performing DPIA in the context of Hospital Information Systems.

## 2. Methods

### 2.1. Methodology development steps

The definition of the methodology follows the steps depicted in Fig. 1. We first performed an analysis and examination of the GDPR and other sources regarding DPIA (Step 1, Fig. 1), with the purpose of identifying the issues related to GDPR application in the healthcare environment. We decided to consider only official and trustworthy documents, published after the adoption of the GDPR (April 14, 2016); in addition to GDPR, the above-mentioned DPIA guidelines [12] published by the Art.29 Working Party and the "Privacy Impact Assessment (PIA)" methodology developed and published by the French data protection [13] authority were analyzed. The results of the analysis led to the identification of the most critical issues related to the HIS environment, which grounded the proposed methodology acting as constraints. Considering these constraints, we then identified the information and documents necessary to assess the data protection risks (Step 2, Fig. 1) and the workflow to follow in order to execute the DPIA in the context of HISs (Step 3, Fig. 1). The workflow was designed in order to show (1) in which part of the hospital processes the DPIA takes place, especially for new software that are purchased or implemented in the HIS, and (2) how to perform the DPIA on the single software. Then, we developed a software allowing the deployment of the proposed workflow (Step 4, Fig. 1). The software was developed using MS Access DBMS and comprised a series of sheets that are used to document the DPIA. Finally, we validated the workflow using the implemented software on a series of software applications running in a real HIS environment (Step 5, Fig. 1), as described in Section 2.3.

### 2.2. Normative framework

Guidelines propose several exemplary methodologies to perform DPIA. Among these, the PIA [13], published by the Commission Nationale de l'Informatique et del Libertés (CNIL, France), proposes a simple and intuitive methodology which is also supported by a dedicated software [14]. The PIA methodological approach grounds on two principles:

- The compliance with normative principles and fundamental rights of individuals. These shall be always guaranteed, independently of the type of data or processing.
- The risk management related to data security, aimed to mitigate the risks associated to an acceptable level.

From these fundamental principles, the DPIA methodology is defined as a 4-step process:

1 Define and describe the context of the considered processing.
2 Analyze the measures that guarantee the compliance to the fundamental principles (art 5, and 13–22).
3 Evaluate risks associated with data security and ensure their proper mitigation measures.
4 Document the formal validation of DPIA.

The risks associated are divided into three unwanted events, corresponding to the three characteristics of information security (CIA). In a risk analysis, a risk level for each of these events shall be quantified, starting from the probability for an event to occur (which depends on the vulnerabilities of the systems involved in the processing) and from the severity of the consequences (which depends on the context of the processing). Therefore, to assess the level of risk for each event, it is mandatory to:

1 Define the potential impact on individuals.
2 Estimate the severity of the impact, with specific reference to the rights and freedom of individuals.
3 Identify the threats that may result in the event, and the sources of risk that may cause it.
4 Estimate the probability for an event to occur.

The residual risk is calculated starting from the risk assessment, and applying the mitigation measures.

### 2.3. Case study and validation

We applied the methodology to the assessment of 11 IT software devices already in use or intended to be used at the Azienda Sanitaria Universitaria Giuliano Isontina, which is a public healthcare enterprise in Friuli-Venezia-Giulia Region in Italy serving the Trieste and Gorizia area which has nearly 300.000 inhabitants. Its duties are heterogeneous and include both highly specialist acute hospital care and province wide territorial healthcare services (such as home care, prevention and vaccines).

In the enterprise, more than 100 software applications are used to deliver such services, together with some tens of new medical equipment installed or substituted every year. Moreover, the Friuli-Venezia-Giulia Region requires the use of public bids to supply both software and medical devices, mostly based on lower prices, with less attention to information security guidelines.

Therefore, we assume the ASUGI scenario to be representative of a typical public healthcare environment and worthy to be studied for the application of state-of-art DPIA procedures, which, as we will see, are not targeted to healthcare sector.

## 3. Results

### 3.1. Definition of critical issues

#### 3.1.1. Critical issue 1: the definition of processing

According to the GDPR, the DPIA shall be performed on a single processing, or on a set of similar processing resulting in similar risks. Therefore, one or more processing defined in the ROPA are the subject of the DPIA (if they result in high risks).

In healthcare, there may be multiple definitions of "processing": it can refer to a specific care pathway, or to a whole ambulatory setting, or to a single diagnostic examination for a single patient.

The ISO/IEC 29134:2017 [15], which is cited in the WP248 [12] guidelines as reference for DPIA, allows focusing on an information system instead of focusing on a single processing. This standard defines the PIA as a tool to evaluate potential impacts to the privacy of a process, information system, software, software module, device, or entity processing personal data [15].

The critical issue of precisely identifying the subject of the DPIA (the "processing") can be overcome according to this standard by focusing on the information system that processes the data. In fact, the major risks reside in the data flows involving electronic transmissions that treat a large amount of data and can be subject to unwanted access.

#### 3.1.2. Critical issue 2: compliance to the rights and freedom of individuals

In healthcare, it is well-known that one of the most important characteristics of data is that the data owner (the patient) is different from the data user (the healthcare professional). Therefore, not all the rights composing the basic principles of PIA (as defined in art 13–20) can be applied to all health-related data. Healthcare institutions already provide some rights to patients in terms of data accessibility and portability, wherever possible, but not, for instance, the right to delete data, which is forbidden by law. Regarding accessibility (art15), patients usually have the right to request copy of their healthcare data (health records, reports, etc.), but do not have the right to access any data at any time, as conversely do healthcare professionals who are in charge to treat the patient. Regarding portability (art 20), this is subject to the availability of standards ensuring system interoperability, thus limiting the type of portable data (e.g., diagnostic images using DICOM are portable whereas records not complying with HL7-CDA2 are not).

For these reasons, it is impossible to apply Step 2 (Definition of the measures that guarantee the compliance to the fundamental principles) of the PIA methodology to healthcare data, and therefore this was excluded from the methodology that we developed. The measures that guarantee the compliance to the fundamental principles can be treated in a separate analysis, and only to those data and documents for which they are applicable.

The technical sheet will therefore document only the risk evaluation related to data security, as described in Step 3 of the PIA methodology, although a robust data security will help to accomplish the principles.

#### 3.1.3. Critical issue 3: impact to individuals

In defining the impact to individuals, the PIA methodology defines three types of impacts: physical, material, and psychological. In general, the impact to individuals is difficult to estimate since it depends on the subjective perception of the damage. In addition, health data loss may impact an individual's health: for instance, losing a radiological image may cause repeating the examination, thus increasing the level of ionizing radiation administered to the individual, or, in the case of an emergency, the time lost to repeat the examination may be crucial for the intervention. These types of impacts cannot be fully considered in the DPIA analysis, since they are too specific for the context of the single piece of information, and may be included in the "Information Business Continuity Plan". The latter, which is a mandatory document for public health institutions running internal digital services, should assess the potential damage of each loss of Enterprise Services and provide

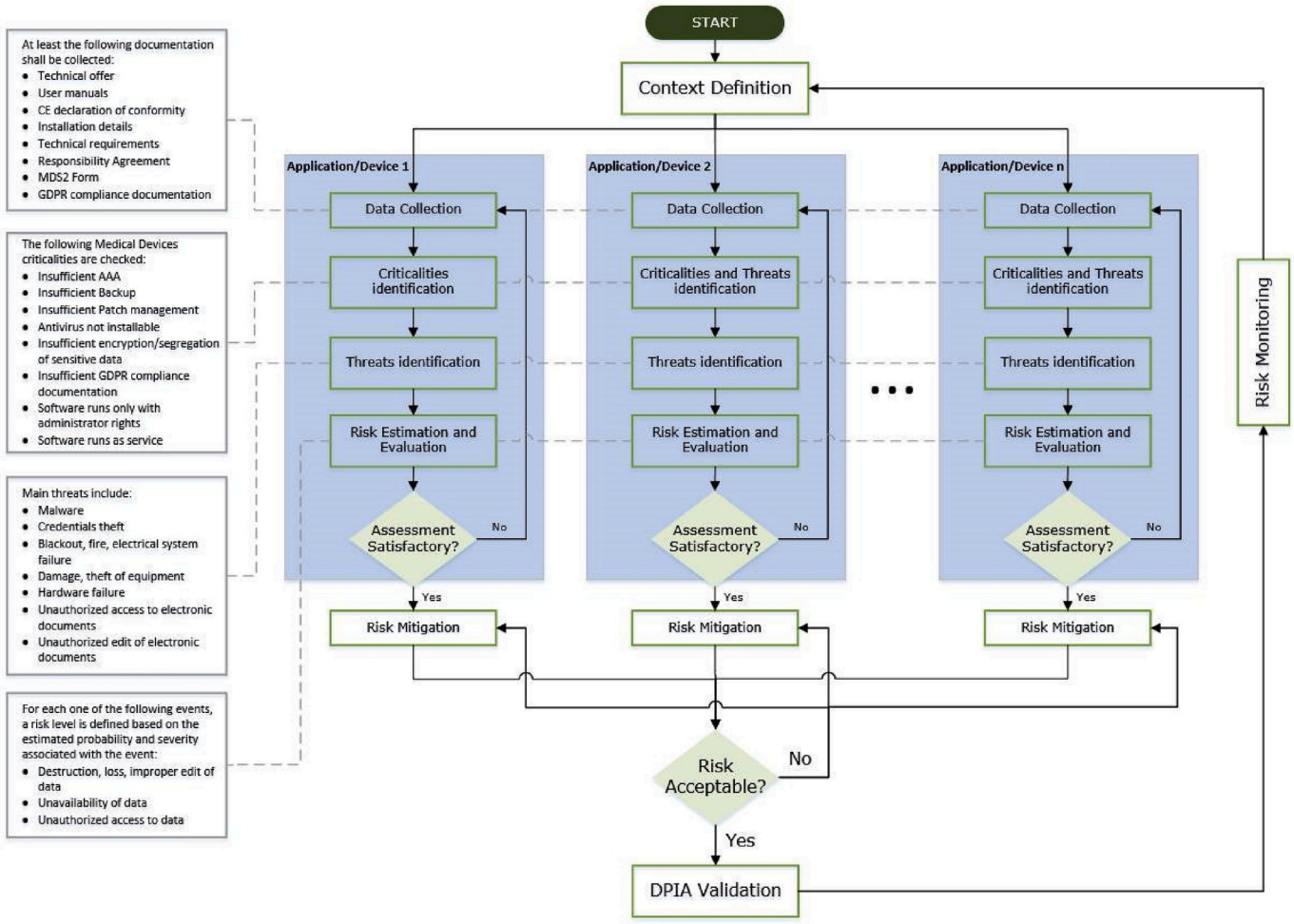


**Fig. 2.** Workflow of information collection for the Data Protection Impact Assessment.

adequate measures, on the technical and economical level, to mitigate the effects of loss of service.

### 3.2. Definition of the information to collect

In general, the subject of a risk assessment can be an information system supporting clinical activities, such as a system supplied after a public bid, that may include different devices with a common aim (e.g., a laboratory system), or a series of different devices with similar characteristics (e.g., a series of ultrasound scanners). In choosing the subject of the evaluation, there is a trade-off between applying a rigorous and systematic approach and the complexity of the evaluation, the sustainability, and the applicability of the evaluation process.

In any case, for each Application/Device that composes the system, all the relevant documentation are collected to serve as a starting point for risk analysis. The reference documentation can be completed starting from the documentation of the technical offer, as well as using manuals, CE declaration of conformity, installation details, technical requirements as defined in the terms of contract, Responsibility Agreement, MDS2 and GDPR compliance. It may be necessary to contact the manufacturer in order to obtain specific details on the mitigation measures implemented.

### 3.3. Workflow to execute the DPIA

We propose to perform the DPIA on a system using a modular approach targeted to the technological asset and not to the processing *per se*: for each information system we propose to create a technical folder aimed to assess the risks associated with that system, and composed of technical sheets, one for each device or module composing the system itself. In other words, we propose to perform the system DPIA starting from the analysis on each single technological asset that is included in a system (single technical sheets), and combine them in a technical folder of the system under DPIA (technical folder), in order to re-use the technical sheets in case the same asset is involved in another context. This has the advantage of being applicable to all of the processing managed by the same technological system, thus making them independent in a many-to-many relation: each processing can be associated with one or more technical sheets, and each technical sheet can be associated with one or more processing.

#### 3.3.1. Workflow for DPIA description

Fig. 2 shows the proposed workflow for the execution DPIA process on a system, which is composed of different Application/Devices.

The starting point of the DPIA is the security model of the healthcare institution, to which each system/device should comply in order to ensure risk mitigation. Therefore, the workflow starts with the definition and description of the context of the processing; this can include technological, organizational, and legal aspects that can influence the process.

Then, for each Application/Device that composes the system, a technical sheet is defined by implementing a risk analysis, starting with the collection of all the relevant documentation. The technical sheet has to evaluate the information system in the context of the institution in

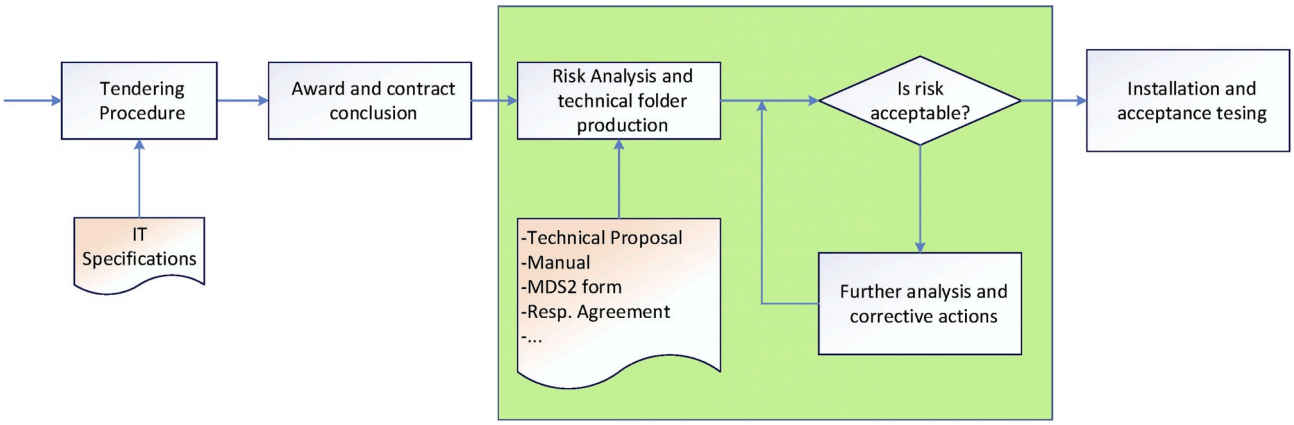


**Fig. 3.** Integration of single application/device assessment in hospital procurement processes.

which it is implemented, more than the security of the system *per se*, because the system or device, when connected to a hospital network, may result in risks other than those identifiable for standalone solutions, as described in IEC 80001-2 [16].

After the identification of the criticalities, along with the threats for the specific Application/Device, a risk level is estimated for each of the three unwanted events (comprising of Confidentiality, Integrity, Availability), based on the probability for the event to occur and on the severity of the impact, with specific reference to the rights and freedom of individuals. If the assessment is satisfactory in terms of comprehensiveness of the analysis, the process continues with the assessment of the proper mitigation measures. Otherwise, after more information is gathered, the analysis for the Application/Device is to be repeated.

When all Application/Devices have been analyzed, in a modular way, the technical folder is created and the overall residual risk of the system composed by all the Application/Devices technical sheets is to be accepted or refused, based on the organization's criteria (e.g. policies, business strategy, risk appetite). In the latter case, further measures are implemented on the Application/Devices in order to reduce the risk of the system. In case the residual risk is accepted, the DPIA is formally documented and validated, and the organization has to manage and monitor the risk throughout the entire lifecycle of the system. Each change in the context shall be analyzed in order to monitor the risks and update the DPIA.

### 3.3.2. *Integration of the workflow in the hospital procurement process*

The evaluation process through technical sheets has to be integrated within the Hospital Procurement Process (Fig. 3).

The technical sheet should be prepared after the system is acquired (usually through a public bid), and before the installation and acceptance testing. This is crucial in order to obtain the necessary changes for mitigating risks before the system implementation.

The installation and acceptance testing shall be performed only if the residual risk is considered as acceptable. Conversely, if it remains not acceptable, corrective measures will be required to the manufacturer and the evaluation will be repeated, until the risk becomes acceptable. The institution should have the right to decline the system installation if the residual risk is judged as unacceptable. In any case, if the IT specifications are well-defined, the residual risk of an unacceptable system is very low.

In the case of a system already in use, the process is the one depicted in the green rectangle (Fig. 3). In this case, the available documentation for the analysis can be insufficient, and the changes needed are less likely to be obtained by the manufacturer (depending on the initial contract).

### 3.4. *Software implementation*

An ad-hoc software developed in MS Access (Microsoft Inc., Redmond, WA, USA) was implemented to support the execution of the proposed DPIA methodology.

The software implemented both the technical folder (system level record) and the technical sheets (application/device level record). The technical folder addresses the evaluation of complex multi-component systems where a comprehensive approach is useful for server-side application, client devices and other connected equipment, and some aspects, like the use case or manufacturer or vendor, are the same. The technical sheet is used to evaluate specific aspects of the single components, such as the way a single device archives sensitive data used in the frame of the system.

The technical folder (Fig. 4) is composed of three different pages. The first one (Fig. 4-A) includes a short description of the system and of the

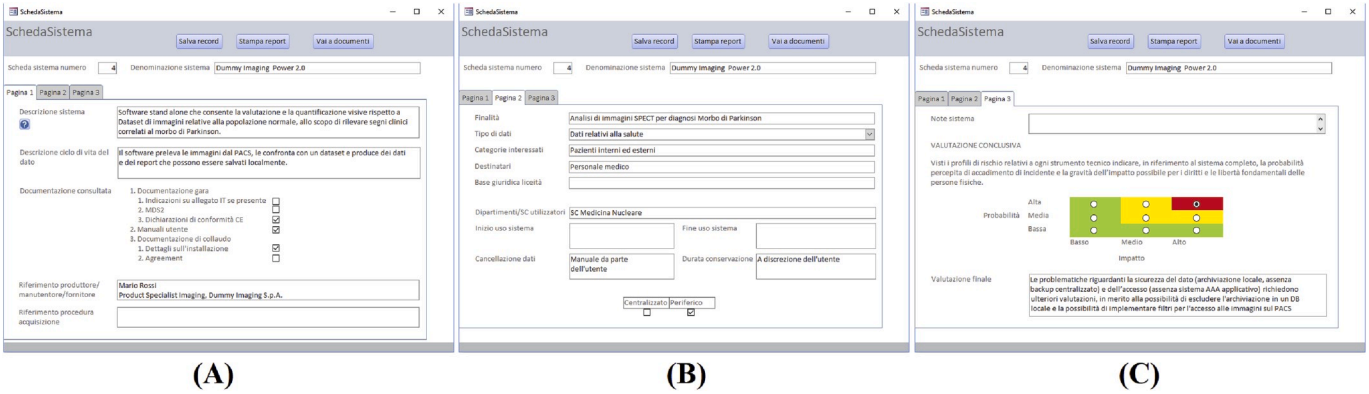


**Fig. 4.** The technical folder (system level record). A- First page. B- Second page. C- Third page.

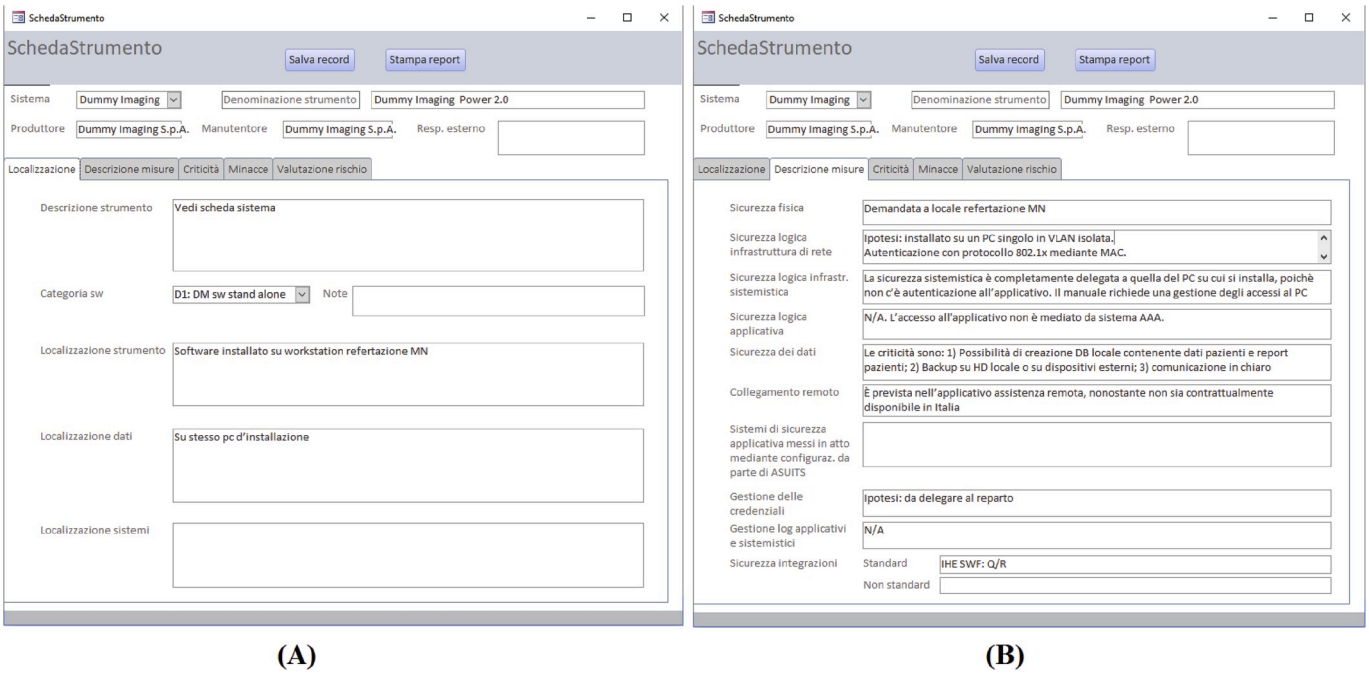


**Fig. 5.** The technical sheet (application/device level record). A- First page. B- Second page.

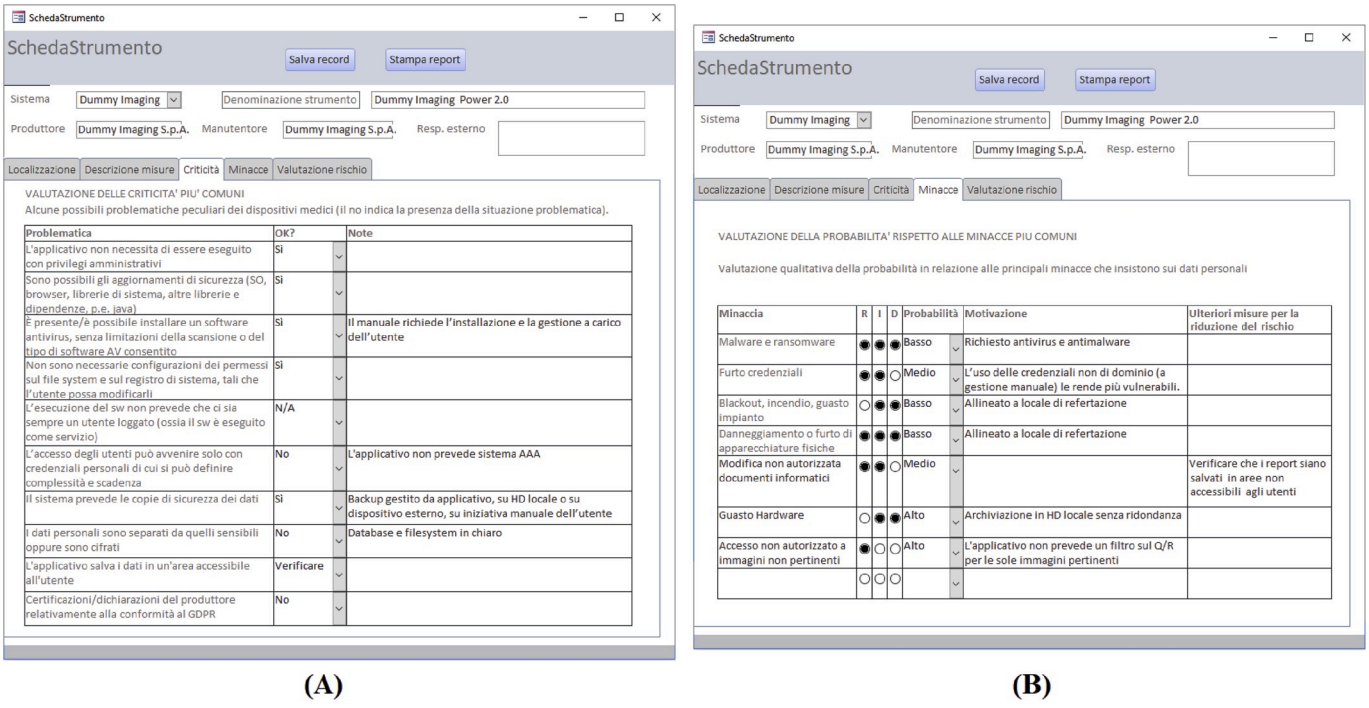


**Fig. 6.** The technical sheet (application/device level record). A- Third page. B- Fourth page.

data life cycle, and a checklist highlighting the reference documentation is used to fill in the record (which is also linked to the record, through the "go to Documents" button on the right top of the page). In addition, it reports the supplier reference, and the reference to the relative ROPA record. This page represents the context definition for the system.

Page 2 (Fig. 4-B) summarizes the information related to the data processing, as defined in the ROPA (e.g., scope, data type, addressee, etc.). The checkbox at the bottom of the page represents the type of integration within the Institutional network, which could be "isolated system" (system that runs on the network but does not share any resources), or "integrated system" (system that shares infrastructural resources with the Hospital Information System, such as Active Directories, Backups, repositories, Virtual Servers, etc.). The third page (Fig. 4-C) reports the probability/impact matrix, and a narrative description of the reasons behind the risk evaluation.

The technical sheet implementing the single application/device record is organized in different pages. The first one (Fig. 5-A) contains the software description, and its classification according to CEI 62-237 guide for medical software [17]. Page 2 (Fig. 5-B) reports a list of the main hypothesized correction measures. For instance, possible at-rest

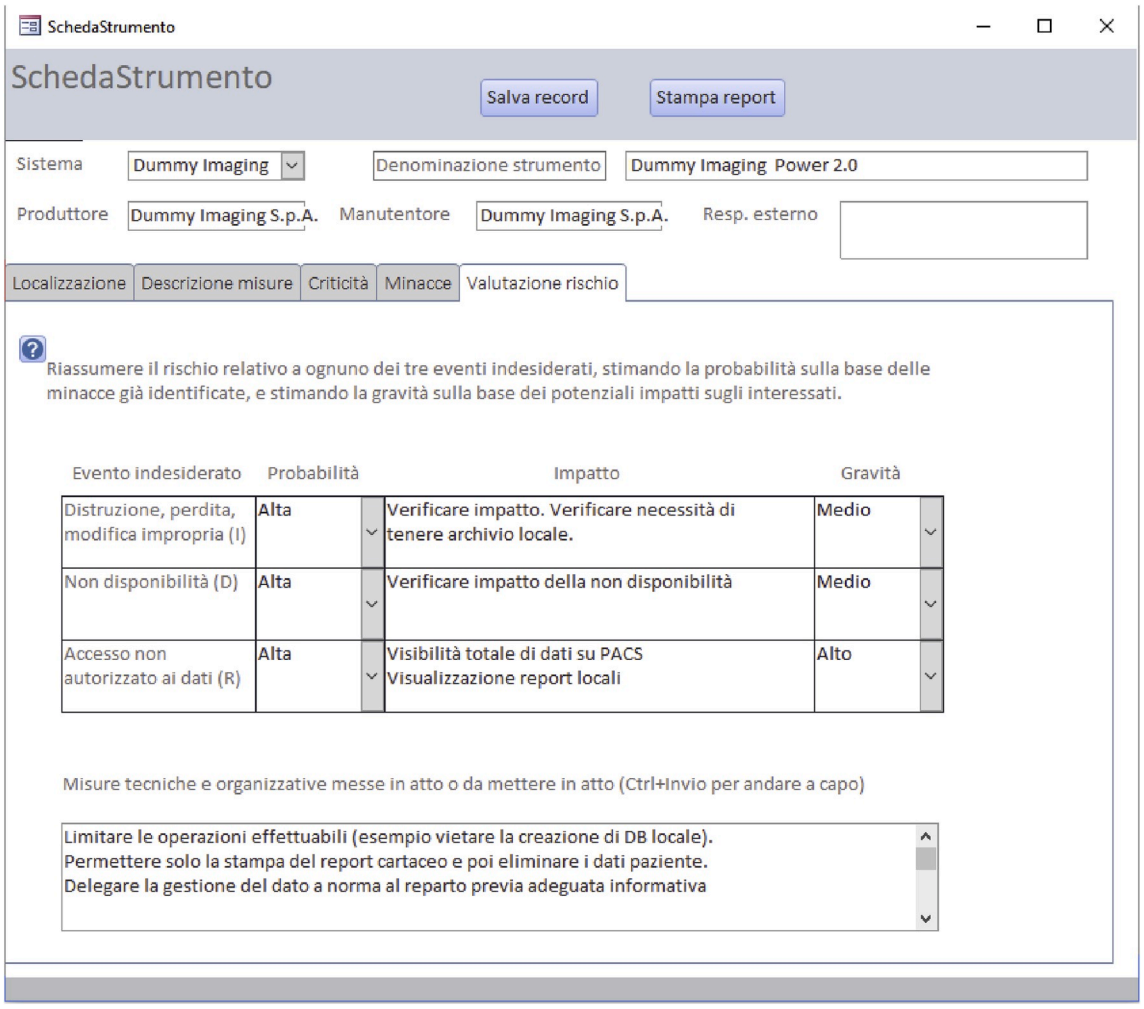


**Fig. 7.** The technical sheet (application/device level record) - Fifth page.

and in-transit encryption features are documented in the "Measures Description" section of the technical sheet (Fig. 5-B) and are considered in the risk estimation and evaluation activity of the workflow (Fig. 2). Page 3 (Fig. 6-A) reports a list of the known possible criticalities of medical software devices, whereas page 4 (Fig. 6-B) reports a table with the identified threats for personal data, each with the estimation of its probability of occurrence. The last page (Fig. 7) documents the risk evaluation related to the rights and the freedom of individuals, according to the realization of the identified threats, and to their estimated probability.

### 3.5. Validation results

The proposed methodology was tested on 11 IT devices in use at the ASUGI. Table 1 reports the results of the risk analysis on each application/device following the methodology proposed for the technical sheet/folder. All the systems were evaluated as Low Risk, except three, which were categorized as Medium and High risk. The major critical issues were the lack of appropriate software security measures (e.g., no authentication or authorization control) or of measures for data safety (e.g., local storage without backup). No further details on the 11 software is provided since we do not intend to provide specific judgments on commercial products.

As an example, we describe the content of the technical folder for a "Standalone application for quantitative analysis of nuclear medicine images", which has already been shown in Figs. 4–7. This is a system composed by a single application and therefore we implemented the technical folder and one technical sheet.

In the first page (Fig. 4-A) we reported the use case for the application: a standalone desktop application which loads DICOM files from the file system and performs some specific calculation producing some reports. Then, the checklist with available documentation is compiled: the specific example is a software under evaluation, so that all the bid documents are unavailable, and in the description of the data workflow, the storage of data on a local folder is underlined. In the second page (Fig. 4-B), the scope of the processing – perform a quantitative analysis of nuclear medicine images – and the people involved: patients with oncologic diseases and nuclear medicine physicians as users – the retention period – depending on users' will - are noted.

The application/device record (Fig. 5) shows that the software is a standalone product classified D1 according to CEI 32-237. The security analysis addresses the storage problems, data archived locally on the PC, and the lack of authentication. The software complies with IHE Profiles. The data security is explicitly demanded to the client host policy totally accounted to the user institution. This assumption seemed immediately unacceptable because the institution security model and policy can be applied, under institution responsibility, if the application can fit the infrastructure and environment. This cannot be given as true in an installation manual.

The last page of the application/device record documents the risk assessment of the device. The event "unauthorized access to data" has been rated as highly probable (because of the abovementioned authentication issues) and has been associated with a high severity impact (since access to reports and PACS images could lead to a

**Table 1**
Testing results.

| System | Application/device | Issues | Risk Evaluation |
|---|---|---|---|
| EEG Management | Server side application | None | Low |
| | Client side application | None | |
| Echocardiography machine | Echocardiography machine | Critical application security, mitigated by restricted functionalities and availability to selected users, and very strict data retention policy | Medium |
| Immunohematology Management System | Middleware | None | Low |
| | Lab testing device | None | |
| PACS | PACS Client | None | Low |
| | PACS Server | None | |
| Specialized digital image processing software with thin client architecture | Server side application | None | Low |
| | Client side application | None | |
| Standalone application for quantitative analysis of nuclear medicine images | Standalone client software | Inadequate data security due to unavailable backup policy and local data storage policy. Inadequate application security due to lack of authentication procedure | High |
| Epidemiologic data processing from several csv sources | Standalone application | Inadequate security to be installed client side due to local storage of SQL database files with uncertain encryption | High |

significant impact to the data subject). Regarding the event "data unavailability", the probability has been estimated as high (because of the local storage) and the severity as moderate; it has been assumed that, due to the purpose of the device (which is the diagnosis of a very slow evolution disease), the only consequence for the data subject is the repetition of the examination.

Back on the system record third page (Fig. 4C), the final evaluation is red because the lack of data protection and authorization makes it really easy to access without authorization sensitive data, and the application could not fit the institution information security model/policy.

## 4. Discussion and conclusions

In this work we described a methodology specific for the HISs able to support the risk assessment, and to perform DPIA. The main contribution of this methodology consists in identifying the information system, and not the processing *per se*, as the object of the analysis. This is crucial in the healthcare environment due to the complexity of the processes involving personal data, which would be otherwise difficult to track. In addition, focusing on the systems/software in the context of the HIS represents a modular approach that allows dealing with the integration of different systems, and with the evolution of the HIS components. In fact, when adding a new software/system, instead of re-designing the whole process, it is sufficient to evaluate the risk and the impact of this new software/system in the light of the HIS.

The methodology was successfully applied in a real environment, thus supporting its validity and capability to highlight risks and criticisms in the available software/systems.

A present limitation is that threats and risks are not standardized or categorized and that the organizational process of managing such methodology was not defined yet. More specifically, in the long term, there should be a specific actor within the hospital organization in charge of maintaining and updating the documentation related to the DPIA and produced using the proposed methodology.

The methodology could be part of the GDPR compliance process, which requires also the evaluation of the compliance to the normative requirements and the warrantee of the subject's rights. The records can be extended including the IEC80001 [16] definition of the Medical IT Network Risk Management File which documents the risk management process for each device connected to the HIS network. However, such extension requires the cooperation with other actors, among which the Clinical Engineering Office, because the norm relates also to the concepts of safety and effectiveness of the systems. Finally, the record could document the implementation of the AgID measures [18], which are a set of controls that Italian public administrations must implement in order to ensure a minimum level of ICT security.

In conclusion, the developed methodology is applicable and sustainable, at least in the short term, and has the potential to be extended to a more general data and system security and safety framework, this grounding the process of ensuring a safer data environment in European hospitals.

## Ethical statement

This research does not include human or animal studies and it does not require ethical committee approval.

## Declaration of competing interest

Sara Marceglia is funder and shareholder of Newronika srl, a spin-off company of the Fondazione IRRCS Ca'Granda Ospedale Maggiore Policlinico and of the University of Milan.

## Acknowledgments and funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. Sara Marceglia is partially supported by the Project HUB-Regione Lombardia POR-FESR 2014–2020 "Pain-RElife: Ecosistema big data sostenibile e integrato per la continuità della cura e il supporto alla decisione dei pazienti con dolore".

## Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.imu.2020.100361.

## 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). http://data.europa.eu/eli/reg/2016/679/2016-05-04. [Accessed 25 November 2019].
[2] Decision of the EEA joint committee No 154/2018 of 6 july 2018 amending annex XI and protocol 37 to the EEA agreement [2018/1022]. http://data.europa.eu/eli/dec/2018/1022/oj. [Accessed 25 November 2019].
[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(2):149–56.
[4] Riba M, Sala C, Toniolo D, Tonon G. Big data in medicine, the present and hopefully the future. Front Med 2019 Nov 15;6:263. https://doi.org/10.3389/fmed.2019.00263.
[5] Ursin G. Cancer registration in the era of modern oncology and GDPR. Acta Oncol 2019 Nov;58(11):1547–8. https://doi.org/10.1080/0284186X.2019.1657586.

[6] Crowhurst N, Bergin M, Wells J. Implications for nursing and healthcare research of the general data protection regulation and retrospective reviews of patients' data. Nurse Res 2019 Jan 23. https://doi.org/10.7748/nr.2019.e1639.
[7] Becker R, Alper P, Grouès V, Munoz S, Jarosz Y, Lebioda J, et al. DAISY: a data information system for accountability under the general data protection regulation. GigaScience 2019 Dec 1;8(12). https://doi.org/10.1093/gigascience/giz140. pii: giz140.
[8] Spencer A, Patel S. Applying the data protection act 2018 and general data protection regulation principles in healthcare settings. Nurs Manag 2019 Jan 16. https://doi.org/10.7748/nm.2019.e1806.
[9] Chryssanthou A, Varlamis I, Sarivougioukas JC, Apostolakis I. Hospital information systems replacement and healthcare quality. Int J Rel Quality E-Health 2012;1(3): 1–12. https://doi.org/10.4018/ijrqeh.2012070101.
[10] Fernández A.P., Sindre G. Software assisted privacy impact assessment in interactive ubiquitous computing systems. In: Pappas I., Mikalef P., Dwivedi Y., Jaccheri L., Krogstie J., Mäntymäki M. (eds) Digital transformation for a sustainable society in the 21st century. I3E 2019. IFIP advances in information and communication technology, vol vol. 573. Springer, Cham.
[11] Dashti S., Ranise S. Tool-assisted risk analysis for data protection impact assessment. In: Friedewald M., Önen M., Lievens E., Krenn S., Fricker S. (eds) Privacy and identity management. Data for better living: AI and privacy. Privacy and identity 2019. IFIP advances in information and communication technology, vol vol. 576. Springer, Cham.
[12] 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". Article 29 Data Protection Working Party; 2017.
[13] https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf.
[14] https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protectionimpact-assesment.
[15] ISO/IEC 29134. Information technology - security techniques - guidelines for privacy impact assessment. 2017.
[16] IEC 80001-1. Application of risk management for IT-networks incorporating medical devices – Part 1: roles, responsibilities and activities. 2010.
[17] CEI 62-237. Guida alla gestione del software e delle reti IT-medicali nel contesto sanitario. Parte 1: gestione del software. 2015.
[18] Circolare n. Misure minime di sicurezza ICT per le pubbliche amministrazioni. 2/2017. AgID.