IOP Conference Series:
Materials Science and
Engineering

PAPER • **OPEN ACCESS**

Robust Privacy Assessment in Transnational Healthcare Systems

To cite this article: C Parretti *et al* 2021 *IOP Conf. Ser.: Mater. Sci. Eng.* **1174** 012015

IOP Conf. Series: Materials Science and Engineering 1174 (2021) 012015 doi:10.1088/1757-899X/1174/1/012015

Robust Privacy Assessment in Transnational Healthcare Systems

C Parretti[1], E Pourabbas[2], F Rolli[1], F Pecoraro[3] and P Citti[1]

[1] Guglielmo Marconi University, Department of Engineering Science, Via Plinio 44 - 00193 Rome, Italy
[2] National Research Council, Institute for System Analysis and Computer Science "A. Ruberti", Via dei Taurini, 19 - 00185 Rome, Italy
[3] National Research Council, Institute for Research on Population and Social Policies, Via Palestro, 32 - 00185 Rome, Italy

E-mail: c.parretti@unimarconi.it

Abstract. Recent developments in Information and Communication Technology have paved the foundations for new forms of collaboration between health systems in different countries. These collaborations allow, on the one hand, to monitor recurrent health emergencies on territories, and on the other hand, they allow national health systems to share information about foreign citizens in transit on their territory. European legislation regarding the processing of personal data places strict constraints on the cross-border transfer of personal data. In this case, companies or organizations, operating on information interchange, must adopt robust mechanisms to verify the adequacy requirements, in order to allow monitoring of security levels, identification of possible intervention actions and preparation of updated security plans for inspection visits required by European standards. In this context, Axiomatic Design allows not only to design medical systems and equipment in compliance with current regulations, but also to provide representations of the design artifact already prepared to implant privacy risk assessment mechanisms. This makes it possible to identify the activities/components to be assessed up to a level of elementary granularity such as to allow risk assessment for the single module. At the same time, the axiomatic approach enables the overall recomposition of privacy violation risks on the basis of a modular representation of the whole system according to the well-known V model scheme. This recomposition allows to build the so-called risk privacy coverage matrix, in order to trace the risk level of the elementary modules, associating them with more and more complex components. In this way, the foundations to build a dynamic monitoring system of the privacy risk level of the system can be defined.

1 Introduction

The recent global health crisis induced by the coronavirus pandemic has brought to the attention of the international scientific community the importance of collaboration between countries in the field of public health. The World Health Organization (WHO) already provides specific communication protocols between the various national health systems and supranational organizations, in order to identify early outbreaks of infectious diseases, monitor endemic situations and define guidelines for intervention [1-3]. International collaborations between countries may concern both the sharing of data for exclusively scientific use, and the provision of information directly attributable to patients in order to allow their health treatment in another country, in case of mobility [3, 4]. This last specificity has always posed relevant questions regarding the respect of privacy and the personal data processing [4]. For this reason, the countries adhering to the European Union have adopted the so-called General Data Protection Regulation 679/2016 (GDPR) [5, 6]. The rules contained therein are binding for all countries in the EU area. This has laid the groundwork to enable the interchange of health information about citizens of member countries [7]. This regulation has impact not only at the level of personal data processing, but also it provides requirements for the design, configuration and evaluation of systems and equipment, which handle personal information [8, 9]. For this reason, European legislators have introduced the concepts of Privacy by design, Privacy by default and Privacy Impact Assessment.

Privacy by design means that the design of a healthcare system must be done in a way that "proactively" eliminates or mitigates issues that may lead to privacy violations [10]. Privacy by default, on the other hand, means that a medical procedure or device must be configured in such a way that its primary mode of operation does not allow a healthcare professional or other party to access information for which they are not authorized [8, 9]. Conversely, Privacy Impact Assessment (PIA) is a risk assessment tool, which involves all organizational and technological aspects that impact the processing of personal data [5]. Therefore, this type of assessment must be contextualized to a specific scenario, in which the system must operate.

In this paper, we will focus our attention on how Axiomatic Design (AD) can guide the design of systems operating interchanges of health information between EU member countries. In particular, our goal is to propose a methodological approach that proactively allows reducing the risk of privacy breaches according to GDPR requirements. Specifically, we will give particular relevance to how AD allows to provide representations of the output design, compatible with the adoption of an evaluation tool such as PIA. Based on these representations, we propose an application scheme of PIA based on the axiomatic decomposition of the functional requirements of the system. The goal is the construction of a risk privacy coverage matrix, which describes the privacy risk map for each component of the system. This matrix becomes a tool for monitoring the level of risk associated with the system. In particular, we illustrate how this methodology can be applied to the case of privacy risk assessment for a process of health data interchange for an Italian patient hospitalized in another EU country.

2 Methodological Approach

End-user desires can be formalized in terms of user requirements (Customers Attributes). They consist of functional requirements (FRs), which represent "what the system must do," and design constraints (CSs), which are limitations on operation. In the specific case of GDPR, these constraints are the rules governing the processing of personal data. Instead, Design Parameters (DPs) constitute "how" the functional requirements are to be executed. The possible relations between FRs and DPs can be also multiple. They can give rise to different combinations, but only some of them are acceptable, as they preserve the independence of the functional requirements. This means that only one-to-one relationships can be candidates to represent an acceptable solution of the system to be designed. In matrix terms, this means that the relevant design matrices must necessarily be square diagonal matrices (uncoupled relation) or triangular matrices (decoupled relation). Only these types of FR-DP relations guarantee the functional independence of FRs requirements. On these evidences, the axiom of independence has been formulated. It allows only a finite number of combinations between FR-DP to be defined as admissible solutions [11]. The information axiom, on the other hand, allows restricting the selection to the design solution with minimal information content, i.e., the solution with the lowest complexity [11]. The application of these two axioms takes on specific characterizations, depending on the particular operational context. In particular, the information axiom lends itself to multiple re-interpretations. In our case, the axiom of information can be interpreted in terms of Privacy Impact Assessment. This means that, design solutions that satisfy the axiom of information, can be assessed against the degree of implementation of GDPR requirements. In other words, this methodological assumption allows implementing the concept of Privacy by Design, i.e., designing a system by proactively considering privacy constraints. However, AD is a top-down design methodology, which is based on the decomposition of the functional requirements of the system. This process is carried out by the designers, down to levels of detail that allow the system to be designed. This allows us, also, to build a robust privacy risk monitoring mechanism. This mechanism follows a V-model implementation process, as shown in Figure 1. According to this scheme, we can distinguish two phases of this model. The first phase of the process consists of the axiomatic design of the system, starting from the decomposition of the user requirements (Customers Attributes). This part has been extensively developed in the literature [11-13]. The second phase starts, instead, with the privacy impact assessment of the single elementary modules. At this point, starting with the interactions between elementary parts, the level of risk is measured for increasingly complex components, until the overall risk is determined. All these steps can be tracked by building a risk privacy coverage matrix.

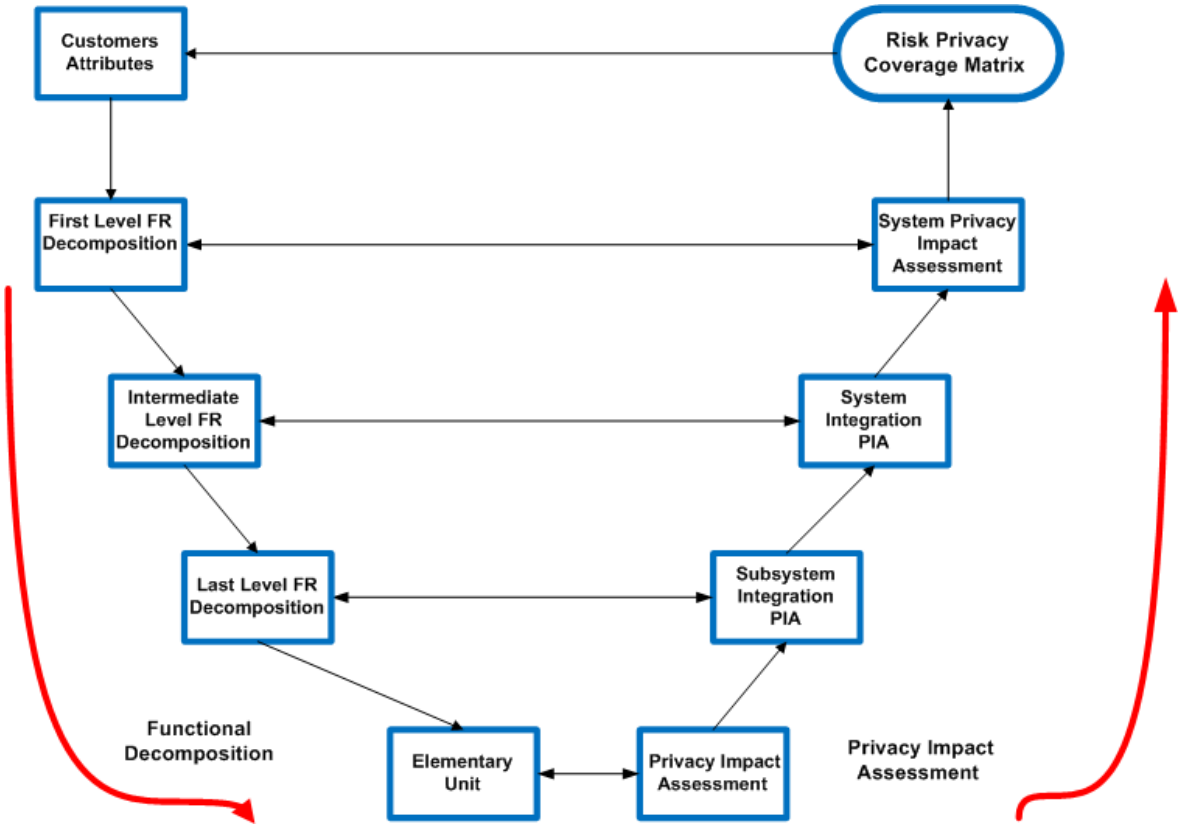

Figure 1 Axiomatic decomposition and Privacy impact assessment

3. Transnational exchange of health data for EU citizens

At this point we can introduce our case study in order to illustrate the application of the proposed approach.

The patient F. C., 65 years old, heart patient, works in Rome but as a dealer of a car company often travels to Greece. Due to his continuous travels, the patient always carries with him an App on his smartphone, where basic clinical data are stored (Patient Summary contained in the patient's medical record). The Patient Summary is generated by the general practitioner by accessing the information contained in his medical record (EHR).

During his most recent stay in Greece, F.C. has an illness and goes to the emergency department of a hospital in Athens. F.C. is conscious. He informs the physician he has the above App available. The doctor, through the data access service on the patient's mobile, views the information contained in the patient's medical record and sees that F.C. has a heart disease. Given the symptoms the patient has at that time, he requests access to F.C.'s additional information such as tests, specialist visits, etc. Thanks to a service offered by the App, after appropriate verification of privacy criteria, the information is directly uploaded from the medical record of the general practitioner. The doctor visits F.C., performs the diagnostic tests to verify the patient's situation and issues the report. The report is then stored on the phone. When F.C. returns to Rome, the general practitioner after examining him, views and stores the Greek doctor's report on his medical record.

In this scenario, therefore, we must take into account the following systems:

- General practitioner's medical record (EHR)
- Patient's personal medical record contained in their mobile (Patient Summary)
- App to access both the patient's personal medical record and the general practitioner's medical record.

3.1 Use-case scenario

The introduced case study can be schematized via UML representations [14, 15]. At this first level of detail, we define a representative form by the use case diagram shown in Figure 2. This representation allows us to define the conceptual design of the system [14]. It consists of the static representation of the system functions (use cases) and the actors operating on them [15]. For this purpose, we can introduce the following use cases:

1. Producing the Patient Summary (PPS). This activity is carried out by the general practitioner who treats the patient in his country of origin. It consists in defining the clinical picture and the therapeutic plan of the patient.
2. Store the Patient Summary (SPS). This use case consists of the GP recording essential health information to be made available in the patient's App for emergency situations.
3. Access the Patient Summary (APS). This use case consists of the Greek hospital center physician accessing summary health information in the cross-border patient's smartphone.
4. Access to Patient Record's (APR). This use case consists of the Greek physician accessing the health information on the cross-border patient's medical record.
5. Access to Italian Health Service (HIS). This use case consists in making available to the HIS the diagnostic and therapeutic information of the patient, treated in Greece.

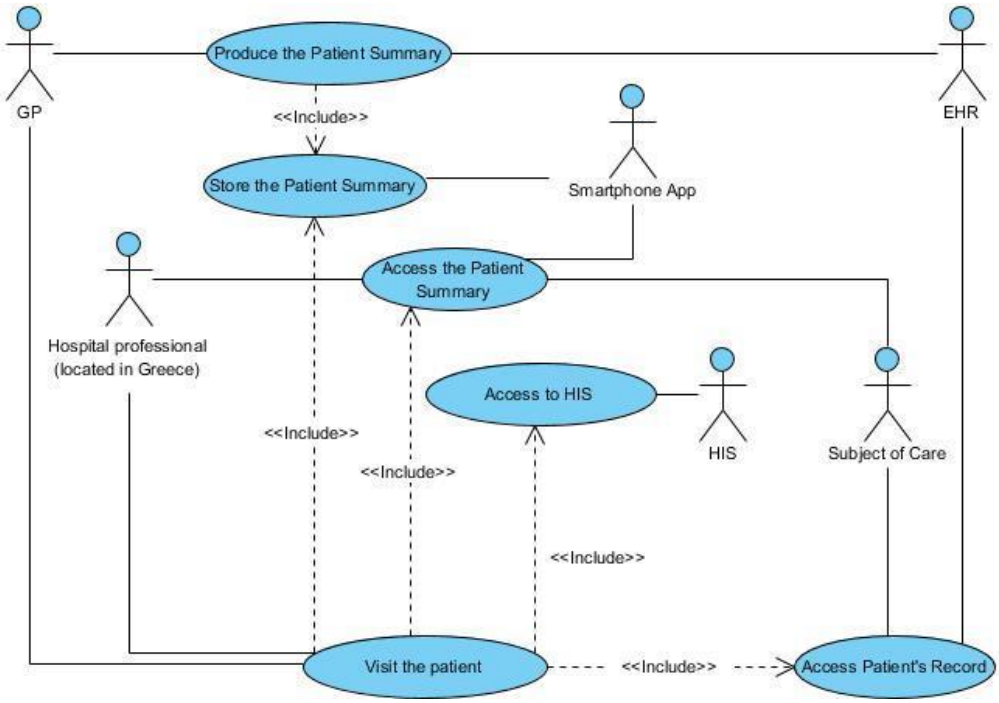

Figure 2 Use case diagram

3.2 Representative forms of the design artifact

For each level of functional decomposition AD provides a representation of the system in terms of design matrix [11]. From the high-level requirements of the system, it is possible to build design matrices representing increasingly detailed design details. This process is carried out to a level of detail sufficient to allow designers to implement elementary modules, which represent specific blocks of the overall design matrix. These modules can be software procedures, electronic components, mechanical parts or even human procedures [16]. AD allows the integrated design of modules of heterogeneous nature. The algebra of matrices, not only allows us to verify the logical coherence of the system, both in terms of functional independence of the individual component parts (Axiom of Independence), and of information complexity (Axiom of Information) [17, 18]. But it also allows us to translate the design matrix, into diagrams consisting of interconnected modules [11, 16]. These representational forms allow privacy impact assessment to be extended from the single elementary module to more complex

structures based on the interactions of elementary components. In this study we will refer to only two levels of abstraction.

3.2.1 Conceptual design of the system

Figures 1 and 3 provide a summary description of the conceptual design of the system. But, in order to proceed to an initial application of AD we need to identify the FRs and DPs of our system. We can pose as FRs the use cases identified in §3.1. Instead, the DPs of the system represent the mutual interactions (collaborations) between the various use cases [12, 19]. Based on these two assumptions, we can provide an initial representation of the system in terms of a design matrix (Table 1). In this case, the relationships between use cases of the system are schematized using the matrix in Table 1. This matrix is constructed by reporting the use cases in Figure 3 along the rows: the functional requirements of the system [12, 19]. Along the column axis, the collaborations (interactions) between use cases are inserted: the high-level interactions between use cases. In terms of AD these are the design parameters of the system and define its behavior. The mapping between FRs and DPs is represented in Table 1 by the symbol X [11]. The cells of the matrix are valorized with symbol X if the use case indicated on the column axis is able to activate a process capable of modifying the state of the target use case [19]. By definition each use case can be modified by its target actor. For this reason, self-collaboration (VP collaboration with respect to VP) is represented in the matrix by the symbol X. As can be seen, the design matrix in Table 1 was constructed on an empirical basis, interpreting the description of end-user desires as given in the previous paragraphs. Our design process is iterative in nature. Therefore, as a starting point, this solution can be considered valid, also because it respects the axiom of independence, since the related design matrix is triangular [11]. With subsequent iterations, following the scheme summarized in Figure 1, we can proceed to improve the conceptual design of the system as well. However, the phenomenon related to sequential coupling will always turn out to remain. This is due to the fact that the activation of the use case FR_{i+1} always depends on the previous FR_i. This is a structural type situation [20]. On the other hand, this type of sequential coupling can be neglected because the relationship between FR-DP is of decoupled type. For simplicity, we do not apply the information axiom.

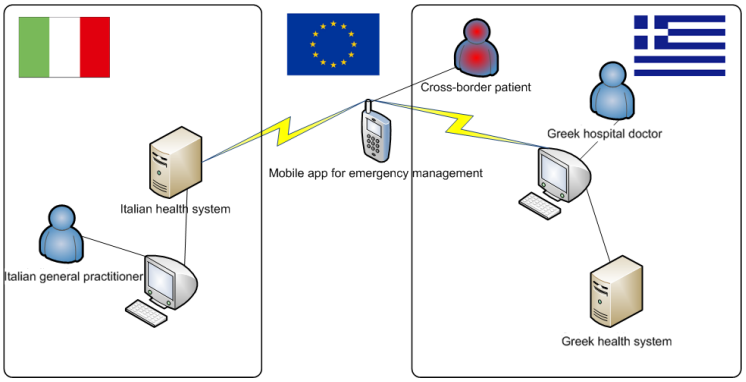

Figure 3 Summary representation of the mode of acquisition of medical information related to EU patient in emergency in Greece

Table 1. Conceptual system design matrix

	PPS collaboration	SPS collaboration	APS collaboration	APR collaboration	HIS collaboration
PPS	X				
SPS	X	X			
APS		X	X		
APR		X	X	X	
HIS			X		X

3.2.2. Modular representation of the conceptual design of the system

The design matrix in Table 1 can also be represented in equivalent form as a system of equations (eq.1).

$$\begin{Bmatrix} PPS \\ SPS \\ APS \\ APR \\ HIS \end{Bmatrix} = \begin{bmatrix} X & & & & \\ X & X & & & \\ & X & X & & \\ & X & X & X & \\ & & X & & X \end{bmatrix} \begin{Bmatrix} PPS\ col \\ SPS\ col \\ APS\ col \\ APR\ col \\ HIS\ col \end{Bmatrix} \quad (1)$$

This representation is possible because each row of the design matrix in Table 1 is a relationship between DPs and FRs. We can say that every functional requirement FRs is satisfied if there exists a function M (module) such that FR =M (DP). For simplicity of expression we can introduce the operator *. This operator allows us to represent in equivalent modular form the mapping relations (FR/DP), even in cases of non-linearizable systems and at high abstraction levels. In this way, we can use the following simplification: FR =M (DP) = M*DP. This assumption allows us to translate the design matrix of Table 1 into diagrammatic terms. In this context, we have resorted to flow chart diagrams to provide a modular representation of the system. However, before describing the flow chart associated to the system of Table 1, it is necessary to introduce three rules of composition of a modular system from a design matrix.

Rule #1:

If the elements of the design matrix are arranged along a diagonal, the system is said to be uncoupled [11]. These systems are characterized by the fact that the functional requirements FRs are all independent (eq.2).

$$\begin{Bmatrix} FR_1 \\ FR_2 \end{Bmatrix} = [a \quad b] \begin{bmatrix} DP_1 \\ DP_2 \end{bmatrix} \rightarrow \begin{cases} FR_1 = M_1 * DP_1 \\ FR_2 = M_2 * DP_2 \end{cases} \quad (2)$$

In this case, the modules of the system can be represented in terms of flow charts as in figure 4. The symbol S stands for the sum relationship of the outputs of the two modules. This configuration corresponds to a parallel connection of the system modules.

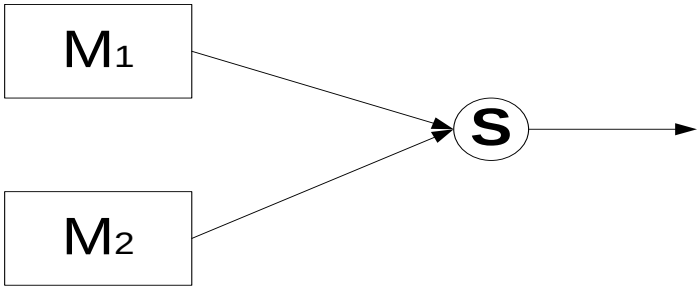

Figure 4
Flow chart diagram for an uncoupled system

Rule #2:

A design matrix of triangular type is defined as decoupled [11]. In this case, the next module always depends on the previous one. In equivalent form, we can say that the modules of the system are connected in series. The following system of equations illustrates this particular configuration (eq.3).

$$\begin{Bmatrix} FR_1 \\ FR_2 \end{Bmatrix} = [a \quad b \quad c] \begin{bmatrix} DP_1 \\ DP_2 \end{bmatrix} \rightarrow \begin{cases} FR_1 = aDP_1 = M_1 * DP_1 = f(DP_1) \\ FR_2 = bDP_1 + cDP_2 = M_2 * DP_2 = f(DP_1, DP_2) \end{cases} \quad (3)$$

where

$$M_2 = b\left(\frac{DP_1}{DP_2}\right) + c \quad (4)$$

In this case, the operation of the system is defined by an ordered sequence of actions. It begins with the M_1 module and progresses to the M_2 module. This means that the output of the module M_1 constitutes the input of the module M_2. Figure 5 shows the graphical representation in terms of flow chart diagram of the system of eq.2.

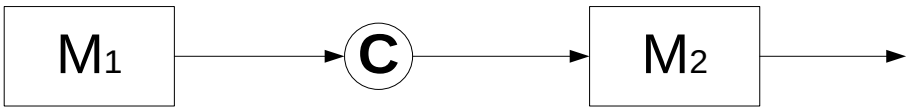

Figure 5 Flow chart diagram for an uncoupled system

Rule #3

A design matrix is called coupled when the functional requirements (FRs) are not independent [11]. In this case the behavior of the system can no longer be represented by simply connecting modules in series and/or in parallel. In order to define the state of the system it is necessary that some modules have an informative feedback (F-Feedback). In these situations, it is said that there is a feedback relationship between the various modules. In matrix terms connections of this type are represented by sparse matrices.

$$\begin{Bmatrix} FR_1 \\ FR_2 \end{Bmatrix} = \begin{bmatrix} a & d \\ b & c \end{bmatrix} \begin{bmatrix} DP_1 \\ DP_2 \end{bmatrix} \rightarrow \begin{cases} FR_1 = aDP_1 + dDP_2 = M_1 * DP_1 \\ FR_2 = bDP_1 + dDP_2 = M_2 * DP_2 \end{cases} \quad (5)$$

Where

$$\begin{cases} M_1 = a + d\left(\frac{DP_1}{DP_2}\right) = f(DP_1, DP_2) \\ M_2 = b\left(\frac{DP_1}{DP_2}\right) + c = f(DP_1, DP_2) \end{cases} \quad (6)$$

In graphical form the system of eq.5 is representable from the flow chart of figure 6.

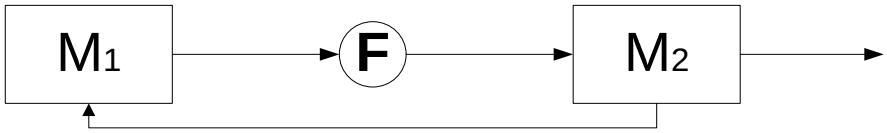

Figure 6 Flow chart diagram for a coupled system

From the previous three rules, the system of equations (eq.1) can be converted graphically in the flow chart diagram of figure 7. Each Mi-th block represents a row of the design matrix of Table 1 [16].

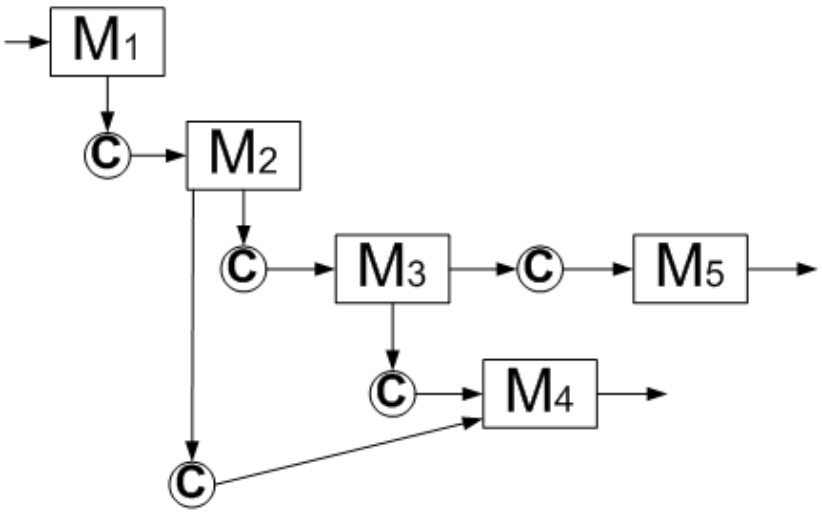

Figure 7 Flow chart of the conceptual design of the system

3.3 Representations of the logical design of the system

AD allows us to continue the functional decomposition of our case study. Starting from the matrix of Table 1 we can obtain, with two successive decompositions, the design matrix of Table 2. It represents in matrix form the logical design of the system and describes the behavior of the system itself in terms of sequence of activities. We can provide a twofold representation of the logical design of the system: dynamic or static. The dynamic representation comes described through translation of the design matrix of table 2 in terms of sequence diagram. In this case our attention is stopped on the sequence of necessary actions in order to define the main behavior of the system. The static representation of the system instead sets to the center of the analysis the activities that come executed in sequence. They come represented in modular shape through flow chart. At this level of detail, the phenomenon of sequential coupling is much more evident. As anticipated in section §3.2.1, it depends on the particular operational context

that involves the sequential activation of the actions constituting the main behavior of the system [20]. However, in this case, this phenomenon can still be neglected because the design matrix of Table 2 turns out to be decoupled. Therefore, the independence axiom is valid.

Table 2 System logic design matrix

			PPS collaboration			SPS collaboration				APS collaboration							APR collaboration						HIS collaboration					
			DPA		DPB	DPC				DPD	DPE	DPF	DPG		DPH	DPI	DPL	DPM				DPN		DPO			
			DP1	DP1.1	DP2	DP3	DP3.1	DP3.2	DP3.3	DP4	DP4.1	DP5	DP6	DP7	DP7.1	DP8	DP9	DP10	DP11	DP11.1	DP11.2	DP11.3	DP12	DP12.1	DP13	DP13.1	DP13.2	DP13.3
PPS	A	1	X																									
		1.1	X	X																								
	B	2		X	X																							
SPS	C	3			X	X																						
		3.1				X	X																					
		3.2					X	X																				
		3.3						X	X																			
APS	D	4								X																		
		4.1								X	X																	
	E	5									X	X																
	F	6										X	X															
	G	7					X						X	X														
		7.1												X	X													
	H	8													X	X												
APR	I	9														X	X											
	L	10														X	X											
	M	11					X										X	X										
		11.1																X	X									
		11.2																	X	X								
		11.3																			X	X						
HIS	N	12														X							X					
		12.1																					X	X				
	O	13																						X	X			
		13.1																							X	X		
		13.2																								X	X	
		13.3																									X	X

3.3.1 Dynamic representation of the logical design of the system

Starting from the design matrix of Table 2 we can obtain a sequence diagram [19]. This particular diagram describes the main behavior of the system as a sequence of actions. They can be human procedures, such as *4: getPatientInfo*. In this case the doctor of the Greek hospital facility accesses, via App of the patient's cell phone, the patient's health information. In other cases, they are automated processes of the system triggered under specific conditions. For such reason this particular diagram previews the indication of the trigger of activation of the action: a stylized man, in the case of human intervention; a rectangle with the indication of the activating system, for the processes started from the system. In figure 8 we have brought back the sequence diagram that describes the dynamic behavior associated to the logical design of the system [15].

3.3.2 Static representation of the logical design of the system

From the design matrix in Table 2, it is possible to represent the top-level modules (M_1, M_2, M_3, M_4, M_5) as distinct systems of equations [11]. From this we have the following equations:

$$\begin{Bmatrix} 1 \\ 1.1 \\ 2 \end{Bmatrix} = \begin{bmatrix} X & & \\ X & X & \\ & X & X \end{bmatrix} \begin{Bmatrix} DP1 \\ DP1.1 \\ DP2 \end{Bmatrix} \tag{7}$$

$$\begin{Bmatrix} 3 \\ 3.1 \\ 3.2 \\ 3.3 \end{Bmatrix} = \begin{bmatrix} X & & & \\ X & X & & \\ & X & X & \\ & & X & X \end{bmatrix} \begin{Bmatrix} DP3 \\ DP3.1 \\ DP3.2 \\ DP3.3 \end{Bmatrix} \tag{8}$$

$$\begin{Bmatrix} 4 \\ 4.1 \\ 5 \\ 6 \\ 7 \\ 7.1 \\ 8 \end{Bmatrix} = \begin{bmatrix} X & & & & & & \\ X & X & & & & & \\ & X & X & & & & \\ & & X & X & & & \\ & & & X & X & & \\ & & & & X & X & \\ & & & & & X & X \end{bmatrix} \begin{Bmatrix} DP4 \\ DP4.1 \\ DP5 \\ DP6 \\ DP7 \\ DP7.1 \\ DP8 \end{Bmatrix} \tag{9}$$

$$\begin{Bmatrix} 9 \\ 10 \\ 11 \\ 11.1 \\ 11.2 \\ 11.3 \end{Bmatrix} = \begin{bmatrix} X & & & & & \\ X & X & & & & \\ & X & X & & & \\ & & X & X & & \\ & & & X & X & \\ & & & & X & X \end{bmatrix} \begin{Bmatrix} DP9 \\ DP10 \\ DP11 \\ DP11.1 \\ DP11.2 \\ DP11.3 \end{Bmatrix} \quad (10)$$

$$\begin{Bmatrix} 12 \\ 12.1 \\ 13 \\ 13.1 \\ 13.2 \\ 13.3 \end{Bmatrix} = \begin{bmatrix} X & & & & & \\ X & X & & & & \\ & X & X & & & \\ & & X & X & & \\ & & & X & X & \\ & & & & X & X \end{bmatrix} \begin{Bmatrix} DP12 \\ DP12.1 \\ DP13 \\ DP13.1 \\ DP13.2 \\ DP13.3 \end{Bmatrix} \quad (11)$$

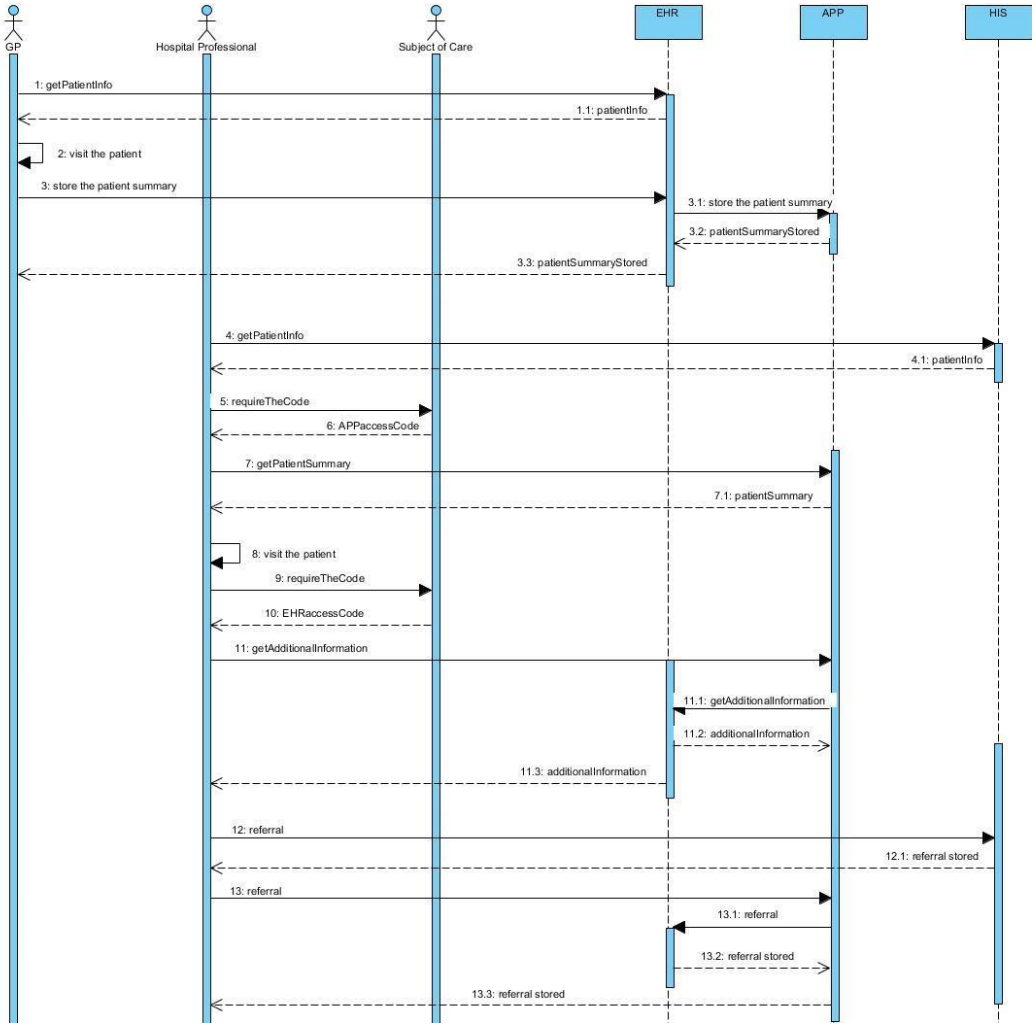

Figure 8 Sequence diagram of the logical design of the system

These equations (eq.7 through eq.11) allow us to treat the top-level blocks as autonomous systems. In fact, we can use the rules introduced in section §3.2.2 to decompose each block into lower level modules. In this way it is possible to construct a flow chart diagram representing the logical design of the system (Figure 9). The blocks M_{ij} are the rows of the matrices referred to the equations from eq.7 to eq.11. This process of modular decomposition can be carried out until identifying the activities or elementary components of the system, on which to carry out the first evaluation of the impact of the privacy

constraints. The recomposition of the level of risk beginning from the elementary blocks follows the rules introduced in section §3.2.2. For this reason, the representation of the system in terms of flow chart allows to build the map of the overall risk level.

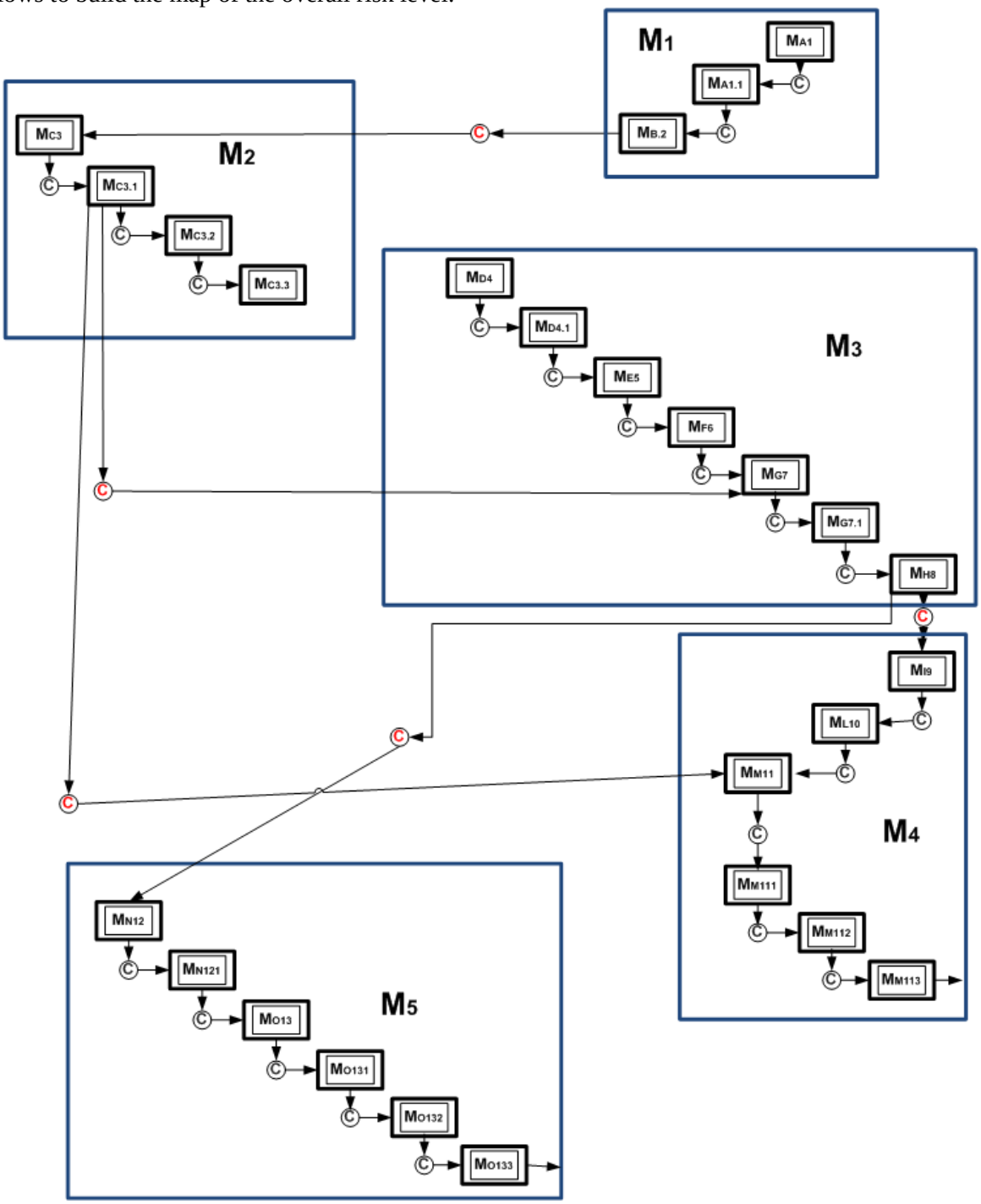

Figure 9 Flow chart diagram of the logical design of the system

4 Elements of the Privacy Impact Assessment plan

The concept of Privacy Impact Assessment, introduced in the European Data Protection Regulation [5], consists in the evaluation and systematic monitoring of the personal data processing that are most exposed to the risk of violation. European legislation has defined three macro-categories of privacy risk [8]:

- Illeg

- al access to data (CS_1);
- Unwanted data changes (CS_2);
- Loss of data (CS_3).

These three macro-categories may represent functional constraints for the AD methodology for the design and subsequent management of the system [11]. In this context, our goal is to build a flexible system monitoring mechanism that allows to estimate the impact of these three constraints in a preventive approach, as it supports software designers in the identification of any critical issues before problems arise. Furthermore, the evaluations criteria defined within the PIA should be adopted to define the overall plan of risks associated with the processing of personal data.

4.1 Modular assessment of the impact of privacy risk

The modular representation of our process allows us to estimate the impact of privacy constraints with respect to individual modules. In this case, to each elementary module M_{ij} we will assign an estimate aij which provides the measure of the impact of the privacy constraint CS_j [8, 9] compute as indicated in the following equation:

$$a_{ij} = S_{ij} + O_{ij} \quad (12)$$

Where S_{ij} represents severity in case of the privacy constraint is violated with respect to the module M_{ij}, while O_{ij} describes the probability that the module M_{ij} does not comply with the constraint CS_j [9, 21].

4.1.1 Severity Assessment

The severity S_{ij} is assessed it is estimated in terms of potential negative impact on the patient deriving from non-compliance with the CS_{ij} design constraint. The values that S_{ij} can assume are integers between 1 and 4, as reported in Table 3 [9, 21]. The determination of these values can be made empirically on the basis of specific check lists [21]. In this regard, please refer to the information provided by the French Data Protection Authority (CNIL) [21].

Table 3. Matrix for assessing the severity S_{ij} [8, 20]

Severity		
Score	**Description**	**Assessment**
1	Negligible	The event did not cause any damage or caused minor inconveniences, such as the recompilation of some forms by the user.
2	Limited	The event caused temporary harm to the patient and necessitated additional interventions (additional costs, stress, temporary suspension of social services, ..)
3	Significant	The event caused temporary damage to the patient, which he should be able to overcome even if with serious difficulties (extension of hospitalization, withdrawal of social services ...).
4	Maximum	The event caused permanent harm to the patient (permanent disability, long-term psychological or physical ailments, death).

4.1.2 Likelihood Assessment

The probability Oij represents the feasibility that the constraint CSij can be violated. It is mainly estimated in terms of the level of vulnerability. The values that Oij can assume are integers between 1 and 4, as reported in Table 4 [9, 21]. The determination of these values can be made empirically on the basis of specific checklists [9]. Also in this case, please refer to the indications provided by the French Data Protection Authority (CNIL) [21].

Table 4. Matrix for assessing the likelihood S_{ij} [9, 21]

Occurence		
Score	**Description**	**Assessment**
1	Negligible	There are no known events.
2	Limited	Documented but not frequent
3	Significant	Documented and frequent
4	Maximum	Documented and very frequent

4.1.3 Risk assessment matrix

The assessment of the risk of a privacy breach is closely related to current legislation. It can only be done on a heuristic basis [21] [22]. Therefore, it is necessary to rely on professionals who are expert in both the legislation and the context in which the system must operate [22]. In this study, as anticipated in the previous sections (§4.1.1 and §4.1.2), we rely on the guidelines prescribed by the French Data Protection Authority (CNIL) [21]. This Authority prescribes a fairly rigorous evaluation process. It is based on personal expert judgments, but is in line with the requirements of the GDPR. As we have already seen, these judgments allow us to assess the level of severity of a privacy breach and the likelihood of it happening. In addition, the Authority itself provides guidance on how to aggregate the two types of ratings. In this case, it provides a two-dimensional representation of privacy risk based on a risk matrix as shown in Figure 9 [21]. Each coloured cell represents a specific risk level. This matrix allows to estimate the privacy risk level of the elementary blocks M_{ij} in Figure 8. By re-aggregating the elementary blocks (M_{ij}) into higher level blocks (M_i) we will be able to attribute the risk level to increasingly complex components. The process will end when the overall level of the process is estimated. This type of matrix is widely used in healthcare, as well as for other types of risk because it has the advantage of being easy to use [22]. However, it can be ambiguous and lead to misleading assessments [23, 24]. For this reason, approaches have been proposed based on quantitative measures of the type of risk to be assessed [24]. Unfortunately, such approaches are not applicable to privacy risk assessment, because the assignment of a value judgment cannot be correlated with quantitative measures. In this case, as already mentioned in sections §4.1.1 and §4.1.2, the various EU authorities propose a series of checklists, so as to allow the attribution of a balanced judgment [9, 21]. However, the combination of the PIA method with AD allows reformulating and refining the value judgments attributable in the first instance, due to the iterative nature of the whole process, as schematized in Figure 1.

Colored cells are the risk privacy categories		Low risk	Limited risk	Significant risk	Maximum risk
		Severity			
		Negligible (1)	Limited (2)	Significant (3)	Maximum (4)
Likelihood	Negligible (1)	2	3	4	5
	Limited (2)	3	4	5	6
	Significant (3)	4	5	6	7
	Maximum (4)	5	6	7	8

Figure 10. Risk assessment matrix

4.2 Risk privacy coverage matrix

The flow chart diagram reported in figure 9 does not only allow us to estimate the privacy risk of the single elementary module, but also to build the risk privacy coverage matrix. This matrix correlates the estimate of the single elementary module, with the higher level component of which it forms part. In this way, the privacy risk can be tracked throughout the process. As shown in Figure 1, the privacy impact assessment is carried out first on the elementary modules. Then, progressively proceeding along the right side of the V model of Figure 1. Thus, an estimate of the higher level module is provided. In this study, the attribution of values is carried out on an empirical basis as suggested by the CNIL [21]. Let's take as an example the module ME5 (RequiretheCode) shown in Figure 8 that corresponds to the request of the Greek doctor to the patient to have the access code to his smartphone. The patient is assumed to be conscious. This action is evaluated with respect to the three situations of privacy violations already introduced (section §4):

A. The CS_1 constraint consists in preventing unauthorized access to the patient's health information management App. In our case, the patient could lose the access code to the medical App of his Smartphone or the code could be used by an unauthorized person. Empirically, a maximum risk level (4) and a significant probability of occurrence (3) has been attributed to a possible violation of this type. Therefore, the level of risk associated with the constraint $CS_1 = 4 + 3 = 7$. If we consider the values of the risk assessment matrix, we have that the risk related to CS_1 has a maximum value. In the risk privacy coverage matrix, the cell corresponding to row ME5 and column CS_1 has the value 7.
B. The CS_2 constraint concerns the possibility that the Greek hospital doctor carelessly modifies the system data. For the M_{E5} module this risk is zero, because it involves requesting a code. No data writing or modification operations are allowed on the system. Empirically, a negligible level of risk (1) and a negligible probability of occurrence (1) have been attributed to a possible violation of this type. Therefore, the level of risk associated with the constraint $CS_2 = 1 + 1 = 2$. If we consider the values of the risk assessment matrix, we have that the risk related to CS_2 has a minimum value. In the risk coverage matrix, the cell corresponding to row M_{E5} and column CS_2 has the value 2.
C. The CS_3 constraint represents the possibility that operations performed by the Greek hospital doctor lead to data loss in the system. This risk is zero, because the ME5 module consists only of requesting the access code to the App of the cross-border patient's smartphone. No data writing or modification operations are allowed on the system. Empirically, a negligible level of risk (1) and a negligible probability of occurrence (1) have been attributed to a possible violation of this type. Therefore, the level of risk associated with the constraint $CS_3 = 1 + 1 = 2$. If we consider the values of the risk assessment matrix, we have that the risk related to CS_3 has a minimum value. In the risk coverage matrix, the cell corresponding to row ME5 and column CS_3 has the value 2.

For each module Mij, the total level of risk is the total risk level is equal to the maximum value of the risks related to the three privacy constraints introduced (CS_1, CS_2, CS_3).

Thus: $a_{ij} = max_{i=1}^{n=3}(S_i + O_i)$

Similarly, the privacy risk value of the higher-level M_i module is equal to the risk value of its higher-rated sub-module (Mij). If we consider figure 9, the M_3 module assumes the risk level of its M_{E5} sub-module, since it has the highest risk value compared to the other sub-modules. Following this reasoning, it is possible to construct the risk privacy coverage matrix of figure 11.

Risk coverage matrix		CS_1	CS_2	CS_3	a_{ij}	A_i
		S_1+O_1	S_2+O_2	S_3+O_3	$a_{ij}=max(S_i+O_i)$	$A_i=max(a_{ij})$
M_1	M_{A1}	2	2	2	**2**	**3**
	$M_{A1.1}$	2	2	2	**2**	
	M_{B2}	3	2	2	**3**	
M_2	M_{C3}	2	3	3	**3**	**3**
	$M_{C3.1}$	2	2	2	**2**	
	$M_{C3.2}$	2	2	2	**2**	
	$M_{C3.3}$	2	2	2	**2**	
M_3	M_{D4}	2	2	2	**2**	**7**
	$M_{D4.1}$	4	2	2	**4**	
	M_{E5}	7	2	2	**7**	
	M_{F6}	6	2	2	**6**	
	M_{G7}	5	2	2	**5**	
	$M_{G7.1}$	5	2	2	**5**	
	M_{H8}	3	2	2	**3**	
M_4	M_{I9}	7	2	2	**7**	**7**
	M_{L10}	6	2	2	**6**	
	M_{M11}	4	2	2	**4**	
	$M_{M11.1}$	4	2	2	**4**	
	$M_{M11.2}$	7	2	2	**7**	
	$M_{M11.3}$	7	2	2	**7**	
M_5	M_{N12}	3	7	6	**7**	**8**
	$M_{N12.1}$	2	2	2	**2**	
	M_{O13}	3	8	7	**8**	
	$M_{O13.1}$	3	8	7	**8**	
	$M_{O13.2}$	2	2	2	**2**	
	$M_{O13.3}$	2	2	2	**2**	

Figure 11. Risk privacy coverage matrix

5 Conclusions

The risk privacy coverage matrix makes it possible to trace the level of risk of the various modules of the system. This allows to lay the foundations for building a dynamic mechanism for monitoring the privacy risks associated with the process in question. A mechanism of this type has the great advantage of defining the critical areas of the system in advance, allowing designers and programmers to identify and apply the necessary adaptation interventions before the problems arise. In practice, this is the application of the concept of Privacy by Design provided for by the GDPR. This involves obtaining substantial economic savings, because it is always “better safe than sorry”. But, as far as healthcare facilities are concerned, it guarantees the levels of adequacy of the processing of personal data required by EU legislation. This certificate of adequacy must be checked periodically. It constitutes the essential condition to allow the electronic exchange of health data relating to EU patients. Furthermore, this system is also dynamic, in the sense that the risk levels defined by the risk assessment matrix in Figure 11 can be reshaped on the basis of contingent situations. Moreover, the Covid-19 pandemic has brought to the attention of political decision makers the question of the temporary suspension of some privacy constraints, in favour of public health. Countries that promptly intervene in this sense have made it possible to contain the infections drastically. In this regard, the case of South Korea is very interesting. The South Korean regulatory system has allowed the use of big data and Apps on smartphones to track the movements of citizens who are positive for the virus. However, if this greater flexibility makes it possible to identify areas of potential infections, it makes it not difficult to identify people who are positive for the virus. This means subjecting some people to social stigma, seriously compromising the rights of citizens. An assessment of the impact of the privacy risk based on Axiomatic Design allows, instead, to proactively highlight all the possible effects of particular interventions. This can help public decision makers to consciously guide their choices.

References

[1] World Health Organization (1946), *The Constitution of World Health Organization, International Health Conference held in New York*;
[2] World Health Organization, (2018) *Communicating Risk in Public Health Emergencies*. A WHO Guideline for Emergency Risk Communication (ERC) policy and practice;
[3] World Health Organization, (2016) *Policy Statement on Data Sharing by the World Health Organization in the Context of Public Health Emergencies;*
[4] World Health Organization, (2017) *Policy on use and sharing of data collected in Member States* by the World Health Organization (WHO) outside the context of public health emergencies;
[5] *General Data Protection Regulation, Regulation* (EU) 2016/679 of the European Parliament and of the Council, Official Journal of the European Union;
[6] Enisa, (2016) *Privacy and Security in Personal Data Clouds*;
[7] European Commission, (2017) *Exchanging and Protecting Personal Data in a Globalized World*, Communication from the Commission to the European Parliament and the Council;
[8] Enisa, (2015) *Privacy and Data Protection by Design*;
[9] Enisa, (2017) *Handbook on Security of Personal Data Processing*;
[10] A. Cavoukian, S. Taylor & M. E. Abrams, (2010) *Privacy by Design: essential for organizational accountability and strong business practices*, Identity in the Information Society volume 3, pages405–413;
[11] N.P. Suh, *Axiomatic Design - Advances and Applications*, (Oxford University Press, 2001);
[12] C. Parretti, F. Rolli, E. Pourabbas, P. Citti, (2018) *Axiomatic Selection of Health and Social Care Web Services on the Basis of Use Cases*, the 12th International Conference on Axiomatic Design (ICAD 2018);
[13] P. Pimentel, C. Stadzisz, (2006) *A Use Case based Object-Oriented Software Design Approach using The Axiomatic Design Theory*. Proceedings of ICAD2006 Fourth International Conference on Axiomatic Design, 4:1-8;
[14] G. Booch, J. Rumbaugh, I. Jacobson, (1999) UML *User Guide*, Addison-Wesley;
[15] M. Fowler, (2010) *UML Distilled*, Addison-Wesley;
[16] S.H. Do, N.P. Suh, (2000) *Object-oriented software design with axiomatic design*, Proc. CIRP 49, 278-84;
[17] F. Rolli, A. Giorgetti, P. Citti, M. Rinaldi, (2016) *Information content evaluation to obtain robustness of the management in Italian fiscal process (Part 2): optimization of Italian income certification process of the year 2016*, Proc. CIRP 53, 63-69;
[18] F. Rolli, A. Giorgetti, P. Citti, M. Rinaldi, (2016) *Improvement of the compilation process of the Italian income certifications: a methodology based on the evaluation of the information content (Part 1),* Proc. CIRP 53, 56-62;
[19] C. Parretti, E. Pourabbas, F. Rolli, F. Pecoraro, P. Citti, A. Giorgetti, (2019*) Robust design of web services supporting the home administration of drug infusion in pediatric oncology*, MATEC Web of Conferences (Vol. 301, p. 00013). EDP Sciences;
[20] C.A. Brown, (2006) *Kinds of coupling and approaches to deal with them*, in Proceedings of 4th ICAD2006, The Fourth International Conference on Axiomatic Design, Firenze, June;
[21] CNIL, (2018) *Privacy Impact Assessment-Knowledge Bases;*
[22] NPSA/NHS, (2008) *A Risk Matrix for Risk Managers*, National Patient Safety Administration, National Health Service (NPSA/NHS): London, UK;
[23] L.A. Cox, (2008) *What's wrong with risk matrices?* Risk Anal. 2008, 28, 497–512;
[24] S. Vatanpour, S.E. Hrudey, I. Dinu, (2015) *Can Public Health Risk Assessment Using Risk Matrices Be Misleading?* Int. J. Environ. Res. Public Health, 12, 9575-9588.