Development of a framework to implement a privacy and data protection program in a pediatric hospital

https://doi.org/10.56238/homeIIsevenhealth-020

Nityananda Portellada
Dacyr Dante de Oliveira Gatto
Renato José Sassi

Keywords: Children's Hospital, Privacy and Data Protection, Information Security, LGPD.

1 INTRODUCTION

Scenario

Privacy is an issue in focus in the modern world, since with the advent of the information and knowledge society, access to data has become systematic and mandatory. Access to individuals', companies', and hospitals' data became increasingly restricted, which led to the creation of legislation on privacy and data protection (BOLLIVAR and MONACO, 2020).

From this reality, they created legislations such as the US Health Insurance Portability and Accountability Act (HIPAA) in 1996 in the United States of America, the General Data Protection Regulation (GDPR) in the European territory in 2016 and the General Data Protection Law (LGPD) in Brazil, through Federal Law n. 13,709/2018 (BRASÍLIA, 2018).

Such legislations, especially the LGPD created several mandatory measures for the processing of personal data, such as, for example, the imposition of an essential change in the methodology of companies' work, based on the organizational efficiency of processes, based on privacy and data protection (BOLLIVAR, 2020).

The processes of Brazilian hospitals were no different because they had to adapt to the determinations of the LGPD, being completely revised, since, with the principle of data minimization, there was a paradigm shift from a process focused only on operational results to a process focused on maintaining the basic rights of the data subject. Moreover, the care with the patient's privacy, previously linked only to the medical record, had to be expanded to the whole process (RIVAROLLI and DAL FARRA NASPOLINI, 2023)

The fact is that in children's hospitals the implementation of a privacy program is more challenging than in other environments because children's hospitals have different processes, whether in the form of data collection, existing regulations, since in a children's hospital the data collection will

always involve sensitive data from children and adolescents, which is not the case in a non-pediatric hospital.

This increases the risk inherent in the privacy and protection of the data subjects' data, since the processing of children's and adolescents' data is considered more critical by LGPD, and is even characterized as high-risk processing by the National Data Protection Authority (ANPD, 2022).

Thus, based on the premise built towards the creation of a privacy program, and based on the assumption of characteristics peculiar to hospital organizations, it is necessary to develop a specific privacy framework for children's hospitals, which is not intended to replace the existing ones, but to adapt to the characteristics of these organizations, and due to legal impositions.

Although children's hospitals are seeking compliance with the LGPD there are gaps in compliance as there is no ease of adequacy in using the currently existing models, which fail to handle large numbers of high-risk data, such as data originating from children and adolescents.

The objective of this work was to develop a framework to implement a privacy and data protection program in a pediatric hospital to improve compliance with the General Law of Data Protection. Although there are several ways to implement a privacy program, the framework will focus on decreasing the risk of data processing without hindering the operation.

It is imperative to mention, once again, that such a privacy program, for being inserted in an extremely computerized society and dependent on information systems, depends on a good application of information security and data governance concepts (LEME and BLANK, 2020), to the extent that it is practically impossible to adopt an efficient privacy program without the adoption of good technological practices, which is the intention of the present study.

This research aims to contribute to academia by developing a model framework for a privacy program adapted for pediatric hospitals, so that the results obtained here can be used by other researchers to develop their own methods.

This replicability is important considering that the LGPD has influenced a strong shift in Brazilian hospitals, especially pediatric hospitals, since, with the principles brought in Article 6 of that law (BRASÍLIA, 2018) it was necessary to incorporate information security measures, impose prior consent for data collection in some situations and the minimization of data collection, in antagonism to a pre-LGPD collection that prioritized maximization, absence of consent and disregard for good governance and security practices.

2 PROBLEM

For healthcare organizations, such as hospitals, clinics and hospital laboratories, this need to adapt to the LGPD was no different from other organizations. However, for these organizations, the process is more costly, to the extent that data processing in healthcare organizations is mostly made

up of sensitive personal data, which brings greater regulatory rigidity (BOTELHO and CAMARGO, 2021).

It is important to remember that, under the LGPD, personal data is defined as any information related to an identified or identifiable natural person, that is, any information that allows an individual to be identified, while sensitive personal data is data about racial or ethnic origin, religious conviction, political opinion, membership in a union or organization of a religious, philosophical or political nature, data concerning health or sex life, genetic or biometric data (BRASIL, 2018).

An aggravating factor in this process is that the models that we have for implementing privacy methodologies were not adequately built for the health area, with its own particularities and risks.

This makes it impossible, from a practical point of view, to manage privacy and information security risks, with such methodologies, without impacting the duty of care, or even the continuity of the organization's activities. In a pediatric hospital, this risk is even greater, since, if a conventional methodology is adopted, which for example, limits the treatment of sensitive data from children and adolescents, the organization's mission will be truly unfeasible.

In turn, if the organization, faced with this difficulty, chooses not to implement any privacy program, there will be a substantial worsening of the risk to the owners, patients of this organization, and the organization itself, since there will be, in addition to the regulatory risks of imposition of a penalty by the National Data Protection Authority (ANPD), a high chance of a leak of personal data and unavailability of the hospital environment, with consequences for patient care and reputation, as well as financial and legal implications (STEP, 2022).

Furthermore, if a privacy program is not implemented, the rights of the patients themselves, children and adolescents, will be affected, as they will have potentially exposed health data whose unrestricted knowledge harms the patient. It is also important to point out that the data itself can be used for other purposes, since there is also the collection of a lot of identification material, which can lead to financial scams, fraud, and extortion.

Thus, it is noteworthy that it cannot be admitted, in view of the risks set forth above, as well as the risk of interruption of business continuity, that a pediatric hospital does not implement a privacy and data protection program, turning then to the problem of the type of framework applicable.

Analyzing the ABNT NBR ISO/IEC 27701 (2019) standard, especially in its item 5.4, one notices a preponderance in the planning and risk analysis of information security and privacy comprising the risk to the holders that does not consider the particularity of the pediatric area, since in a hospital of this specialty the treatment of sensitive personal data of children and adolescents is the majority treatment, which would leave detached issues such as contingency systems and other particularities (BOTELHO and CAMARGO, 2021)

In light of this, it is essential that a framework be developed to implement a privacy and data protection program that is prepared to deal with the particularities of a pediatric hospital without abandoning the principles brought by the General Data Protection Law and the good practices of the market.

The purpose of this project is to answer the following research question: "How can a framework be developed to implement a privacy and data protection program in a pediatric hospital to improve compliance with the General Data Protection Law?

3 OBJECTIVE

The ~~overall~~ objective of this work was to develop a framework to implement a privacy and data protection program at a pediatric hospital to improve compliance with the General Data Protection Act.

A data privacy and protection program is paramount in a pediatric hospital because of the need to properly manage the personal data and sensitive personal data of patients in these facilities, thereby also improving the information security of the hospital environment and mitigating the chance of catastrophic events such as data leaks and care impacts.

4 METHODS

This is an experimental research conducted in a medium-sized pediatric hospital located in the city of São Paulo, with about 180 inpatient beds. A literature review was conducted, searching for articles published in the period from 2018 to 2023 . The selected period, considering that the LGPD was approved in 2018, has legal imposition as to data protection only from this year. Moreover, the literature review was conducted in the following electronic databases: Portal de Periódicos Capes, IEEExplore, PuBMed and Scielo, employing the following descriptors: hospital environment, privacy, data protection, General Law of Data Protection (LGPD), risk management, framework, and their respective synonyms in English.

From the literature review, 47 articles were selected based on the following criteria:

-Tackle the topic of data protection in healthcare;

- Refer to privacy and data protection in healthcare;

- Addressing the impact of the LGPD on healthcare;

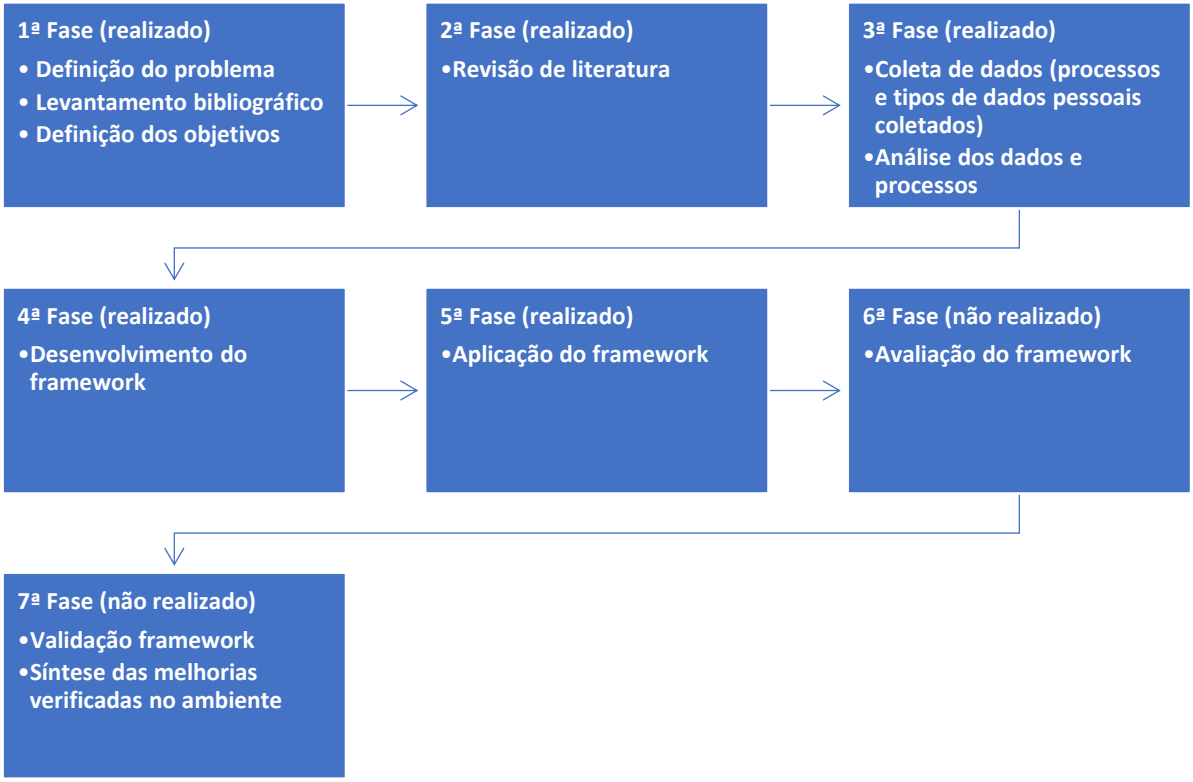
- Have been published in the period 2018 to 2023.

The creation of the framework was proceeded by an analysis of all the processes that handle personal data of the pediatric hospital, being also collected the types of data collected in these processes, being identified the following types of data: Personal Identification Information; Electronic Identification Data; Financial Data; Patient Health Plan Details; Authorization or Consent Data;

Personal Characteristics; Psychological Characteristics; Family Composition; Marriage or current form of cohabitation; Marital History; Residential Data; Academic/School Data; Profession and Employment Data and Sensitive Data of religious conviction, biometrics and concerning health.

The development of the framework was carried out in 7 distinct phases, presented in Figure 1.

Figure 1: Phases of framework development to implement a data privacy and protection program in a pediatric hospital. Source: The Authors.



The following describes the development phases of the framework:

- 1st Phase: Definition of the problem encountered, bibliographical survey, and definition of the objectives of the work, in order to substantiate future development;

- 2nd Phase: Review of the literature found and analysis of the bibliography identified in the previous phase, in order to build the concepts and theoretical foundations of the work;

- 3rd Phase: Collection of the types of personal data handled in the hospital environment, data and process mapping and analysis of the risk identified in each of the mapped processes. Elaboration of the recommendation plan for the organization's adequacy;

- Stage 4: Based on the recommendation plan and the data collected, a replicable framework is developed for other pediatric hospitals;

- 5th Phase: Application of the Framework in the organization and adoption of the indicated measures;

- 6th Phase: Evaluation of the results arising from the application of the framework; and;

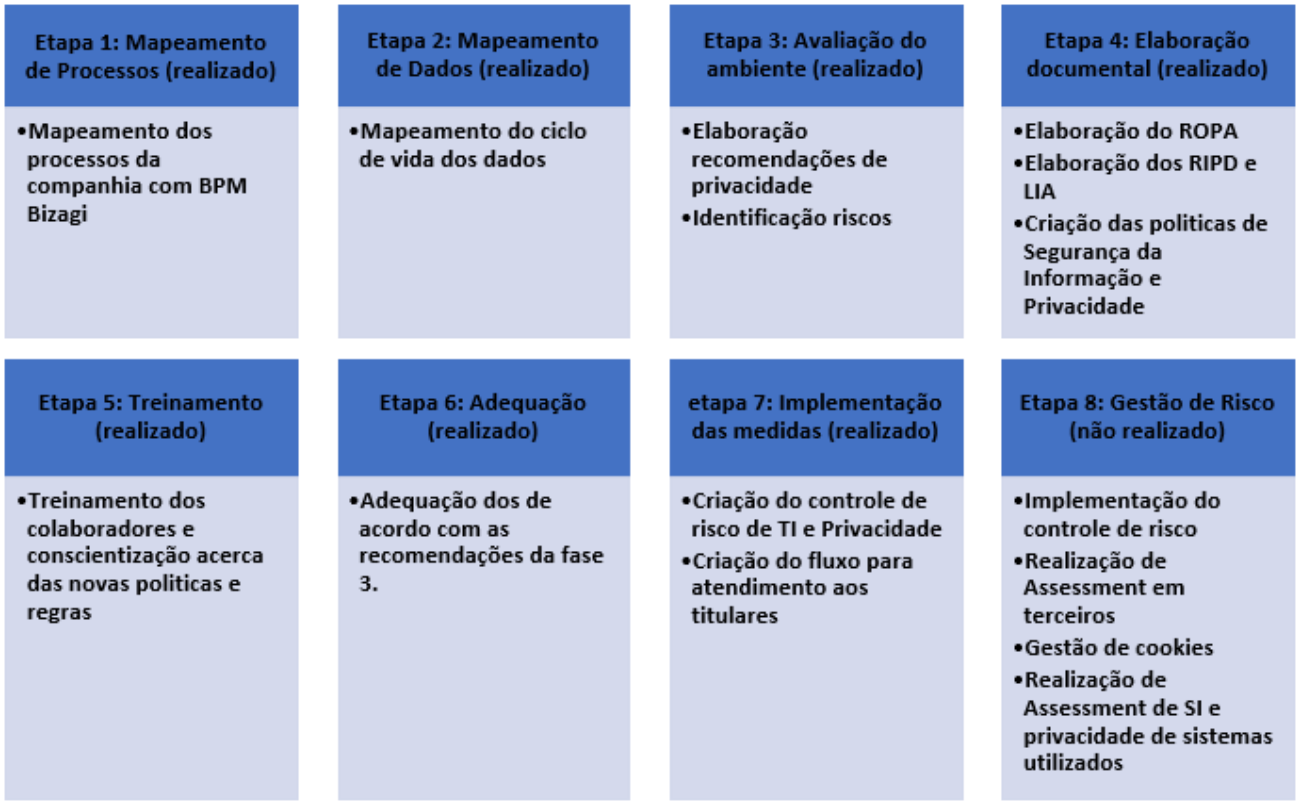
- 7th Phase: Validation of the results and indicators and synthesis of the improvements found.

In turn, phases 3, 4, and 5 were subdivided into stages for the correct analysis of the environment, development of the framework, and its implementation in the hospital. Phase 3 is composed of the following steps: Process mapping; Data mapping and Environment assessment.

Phase 4 is composed of the following steps: Document preparation and employee training. Finally, Phase 5 consists of the following steps: Adequacy of processes; Implementation of improvements and Implementation of risk management.

Figure 2 presents the eight steps of implementing a data privacy and protection program in a pediatric hospital.

Figure 2: The steps of implementing a data privacy and protection program in a pediatric hospital. Source: The Authors.



The work is in phase 5, Application of the framework, and will be evaluated based on the following items:

a) Mapped Processes: Processes of the pediatric hospital that were identified and redesigned with Business Process Model and Notation notation (BPM CBOK, 2014)

- ROPA (Record Of Processing Activities), where the pediatric hospital's personal data processing activities are recorded, as well as the motivation for the processing to occur, its legal basis, the data retention period, and the risks inherent in this processing.

- Policies: Rules and regulations, addressing privacy and data protection issues.

- Risk exposure: Total risk of the pediatric hospital, calculated based on data mapping and analysis of ROPAs.

It is noteworthy that so far the first 5 stages, shown in Figure 1, have been carried out, and that the first 7 stages of implementation, shown in Figure 2, have been carried out.

5 RESULTS

After applying the framework and the steps, it was identified that the pediatric hospital has processes that are supported by critical data, such as the results of infectious and contagious diseases of children and adolescents, pathology diagnoses of children and adolescents, which are often not protected in the correct manner, which, by default, means a significant risk for the organization, so that it became imperative to create a privacy and data protection program. After the implementation of the developed framework, it was observed a qualitative security gain, a systematic review of processes, and a concrete decrease in the existing risk, being mitigated welfare and corporate impacts.

Regarding the pediatric hospital process management, there was a situation in which the processes were not mapped, for example, the patient discharge process, and each area did not have formalized its activities and its sub-processes that would lead to the official conclusion of this activity, which hindered the progress of the work, especially when a responsible person left, who took his knowledge with him. After the beginning of the implementation of the privacy and data protection program, 439 processes were mapped, with the formalization using the PMBOK (PMI, 2021) methodology.

With regard to the management of processes that handle personal data, and the risk management of each of these processes, a Data Treatment Register (ROPA) was developed for each of the 337 processes that collect, produce, receive, classify, use, access, reproduce, transmit, distribute, process, archive, store, delete, evaluate, or control personal data.

Several policies were developed to improve the governance environment, among them, information security policies, privacy policy, clean desk policy, access control and management policy, backup policy, incident management policy, among others, totaling 23 new policies and reform of the 3 previously existing ones.

Table 2 shows comparing the summarized results before implementation and after implementation of the framework.

Table 2: Comparison of summarized results before implementation and after implementation of the framework. Source: The Authors

	Before implementation	After implementation
Mapped Processes	0	439
ROPAS	0	337
Policies	3	26
Risk Exposure	30%	23,75%

By comparing the risk analyses carried out before and after implementation, it was possible to verify that the pediatric hospital's risk exposure was mitigated by about 20%. In addition, it was verified that the organization went through a transformation in terms of process management, with the mapping of processes throughout the company.

A customer service channel was built and is currently active, formatted to meet the requests provided for in Article 18 of the General Data Protection Law, and a company-wide registry of data processing operations was instituted.

Validation of the implementation was accomplished by decreasing the pediatric hospital's risk, creating procedural management, and implementing the recommendations for the entire pediatric hospital's suitability to LGPD.

6 CONCLUSIONS

Privacy is an inalienable right granted by modern constitutions, and is increasingly becoming a major factor in an individual's choice when it comes to dealing with companies and entities.

In the healthcare area, where healthcare standards are strict and result from established protocols, data protection becomes an imposing characteristic, given the regulation and the risk encountered. With the implementation of the framework in the hospital environment, a gain in quality and management was noted, with processes having been established and documented, policies concretized, and risks correctly managed, which reduces the chance of catastrophic impact, whether in a leak or in a regulatory penalty.

The objective was met, given the development of a framework for adaptation of a pediatric hospital to the LGPD and implementation of a privacy and data protection program. In turn, the research question was answered in the sense that in order to build and implement a privacy and data protection framework in a pediatric hospital it is necessary to have a deep mapping of processes, efficient risk management, and correct data management.

The limitation identified in this work was the fact that it was developed in an organization that has only one hospital unit. It is understood that organizations with more than one unit will demand an adaptation of the model, given their particularities in terms of personnel, processes, and logical security.

The sequence of the work will be with the realization of the 6th phase, called "Evaluation of the Framework" and the 7th phase, called "Validation of the Framework", as well as the 8th implementation step, which covers the construction of a risk management.

For future works it is intended to conclude the implementation in the pediatric entity and automate, through an expert system, some steps of the implementation, in order to give more agility in the implementation of the resulting framework.

REFERENCES

ABNT - Brazilian Association of Technical Standards. ABNT NBR ISO/IEC 27001 - Information technology - Security techniques - Information security management systems - Requirements. ABNT, 2022.

ABNT - Brazilian Association of Technical Standards. ABNT NBR ISO/IEC 27002 - Information technology - Security techniques - code of practice for information security controls - Requirements. ABNT, 2022.

ABNT - Brazilian Association of Technical Standards. ABNT NBR ISO/IEC 27701 - Information technology - Security techniques - Extension of ABNT NBR ISO/IEC 27001 and ABNT NBR ISO/IEC 27002 to information privacy management - Requirements and guidelines. ABNT, 2019.

ABNT - Brazilian Association of Technical Standards. ABNT NBR ISO/IEC 31000 - Risk management - Principles and Guidelines. ABNT, 2018.

ANPD - CD/ANPD RESOLUTION No. 2, OF JANUARY 27, 2022 - Approves the Regulations for the application of Law No. 13,709, of August 14, 2018, General Law on Personal Data Protection (LGPD), for small processing agents. ANPD, 2022.

ABRAHAM, A., CHATTERJEE, D., SIMS, R.R. Muddling through cybersecurity: Insights from the U.S. healthcare industry. Business Horizons. v. 62, Issue 4, Aug, p. 539-548, 2019. Doi: 10.1016/j.bushor.2019.03.010

ARAGÃO, S., & SCHIOCCHET, T. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. Revista Eletrônica de Comunicação, Informação e Inovação em Saúde, 14(3), 2020. Doi: 10.29397/reciis.v14i3.2012

ARGAW, S.T.; et al. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Med Inform Decis Mak 20, 146, 2020. Doi: 10.1186/s12911-020-01161-7

ALODAYNAN, A. M. and ALANAZI, A. A. A survey of cybersecurity vulnerabilities in healthcare systems. International Journal of Advanced and Applied Sciences, 8(12), p. 48-55, 2021. Doi: 10.21833/ijaas.2021.12.007

BARRETO JUNIOR, I. F. Protection of Privacy and Personal Data on the Internet: The Marco Civil of the network examined based on the theories of Zygmunt Bauman and Manuel Castells. In: DE LUCCA, N.; SIMÃO FILHO, A., DE LIMA, C. R. P.. Law & Internet III: Marco Civil da Internet. 1ed.São Paulo: Quartier Latin, v. 2, p. 100-127, 2015.

BOLIVAR, ANALLUZA ; MONACO, G. F. C. (Org.) . LGPD IN HEALTH. 1. ed. São Paulo: Revista dos Tribunais, v. 1. 431p, 2020.

BOTELHO, M. C., & CAMARGO, E. P. do A. A aplicação da Lei Geral de Proteção de Dados na saúde. Revista De Direito Sanitário, 21, e0021. 2021. Doi: 10.11606/issn.2316-9044.rdisan.2021.168023

BPM CBOK. Guide to Business Process Management - Common Body of Knowledge. ABPMP CBOK V3.0, 2014

BRAZIL. law No. 13.709, of August 14, 2018. General Law of Data Protection. Brasília: National Congress, [2018]. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Accessed on: 07 Apr. 2023.

FERRAZ JÚNIOR, T. S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista Da Faculdade De Direito, Universidade De São Paulo, 88, 439-459. 1993.

JUNIOR, B. J, et al. Revista Ibérica de Sistemas e Tecnologias de Informação; Lousada Ed. E41, (Feb 2021): 232-243.

NUNES, P., ANTUNES, M., SILVA, C. Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. Procedia Computer Science, v. 181, p 173-181, 2021. Doi: 10.1016/j.procs.2021.01.118

PASSO, MARIA Z. L. B. Why Healthcare Needs to Care about Personal Data Protection. RJLB, Year 8 (2022), no. 2, 1301-1317

PMI - PROJECT MANAGEMENT INSTITUTE. A Guide to the Project Management Body of Knowledge and the Standard for Project Management, 7th Edition, Pennsylvania: PMI, 2021.

RIVAROLLI, M. A.; DAL FARRA NASPOLINI, S. H. Privacy and data protection in nosocomials and clinics before the LGPD. Scientia Iuris, [S. l.], v. 27, n. 1, p. 112-128, 2023. DOI: 10.5433/2178-8189.2023v27n1p112-128.

SALGADO LEME R, BLANK M. General Data Protection Law and information security in health care. Cad. Ibero Am. Direito Sanit. v. 9(3), p. 210-224

SHIN, S.; et al. Proposal for a Privacy Impact Assessment Manual Conforming to ISO/IEC 29134:2017. In: Saeed, K., Homenda, W. (eds) Computer Information Systems and Industrial Management. CISIM. Lecture Notes in Computer Science(), vol 11127. Springer, Cham, 2018. Doi: 10.1007/978-3-319-99954-8_40.