BJEDIS Brazilian Journal of Experimental Design, Data Analysis and Inferential Statistics

Federal University of Rio de Janeiro
BJEDIS, Rio de Janeiro, Special Edition, v. 3 (1), 2024.
DOI: https://doi.org/10.55747/bjedis.v3i1.60729
ISSN: 2763-6925

ARTICLE Received 09/11/2023. Revised 30/12/2023. Accepted 20/12/2023. Published 12/01/2024.

Using BPM for Identification and Processing of Personal and Sensitive Data of Donors: Conceptual Framework

Emmanuel Pires[1], Claudio Luiz de Oliveira Costa[2], Igor Leão dos Santos[3], Augusto da Cunha Reis[4], Keicia Pinto[5]

[1]Postgraduate Program in Production and Systems Engineering – Federal Center for Technological Education Celso Suchow da Fonseca - CEFET-RJ
[2]Postgraduate Program in Production and Systems Engineering – Federal Center for Technological Education Celso Suchow da Fonseca - CEFET-RJ
[3]Postgraduate Program in Production and Systems Engineering – Federal Center for Technological Education Celso Suchow da Fonseca - CEFET-RJ
[4]Postgraduate Program in Production and Systems Engineering – Federal Center for Technological Education Celso Suchow da Fonseca - CEFET-RJ
[5]Hemotherapy Service – National Cancer Institute (INCA)

Abstract: The stock of blood bags to serve the population of patients who need to be transfused is one of the main concerns of the Hemotherapy Services of Public Hospitals (PH). The complexity of managing the blood supply chain ranges from attracting blood donors to dispensing blood bags for transfusion. Understanding the chain processes and maintaining the security of personal and sensitive data from donors becomes one of the premises for public health organizations. The research aims to create and apply a conceptual framework that uses Business Process Management (BPM) approaches and concepts to support managing and securing donors' personal data. The adopted method was the literature review based on scientific articles and the use of BPM in constructing the conceptual framework and applying it in a Hemotherapy Service (HS) of a Federal Public Hospital (FPH) in Brazil. By mapping the blood donation process and using the conceptual framework, possible failures were highlighted that could expose the personal and sensitive data of candidates for blood donation that would be in breach of the General Data Protection Law (LGPD). Using the conceptual framework with BPM to model an organizational process facilitates the identification of the vulnerabilities of the personal and sensitive data of the citizen that circulate in this process and disagree with the norms of the Law.

Adherence to the scope of BJEDIS: This research introduces a blood donation process for the HS in a FPH. The objective is to practically apply the conceptual framework proposed here and in related studies. Notably, BPM, a hallmark of Industry 4.0, extends its influence to administrative processes. A Multidisciplinary Working Group (MWG) within the hospital is tasked with enforcing the LGPD through directives. This endeavor aims to establish a compliant business model across the institution, possibly influencing similar HS in other hospitals.

Key Words: Conceptual Framework, Industry 4.0, BPM, DPGL, Information Security, Hemotherapy Service, Experimental design, Data analysis.

*Address correspondence to this author at the Postgraduate Program in Production and Systems Engineering, Federal Center for Technological Education Celso Suchow da Fonseca – CEFET-RJ, Av. Maracanã, 229 – Maracanã – Rio de Janeiro/RJ, Brazil, Box: 20271-110; Tel.: +55-21-2566-3179; E-mails: emmanuel.pires@aluno.cefet-rj.br ;igor.santos@cefet-rj.br, claudioluizoc@gmail.com

DOI: https://doi.org/10.55747/bjedis.v3i1.60729
ISSN: 2763-6925

1 INTRODUCTION

One of the primary challenges faced by Federal Public Hospitals (FPH) in Brazil is ensuring an optimal blood supply to adequately cater to patients in need of transfusions. Furthermore, these hospitals must ensure the seamless operation of their organizational processes, particularly those that encompass a Hemotherapy Service (HS) or Blood Transfusion Service. These services encompass the critical tasks of blood collection, storage, and distribution of blood products throughout their production chain. Within this context, Ordinance 158/2016 (1) plays a significant role as it outlines the Technical Regulations for Hemotherapy Procedures. Article 1, paragraph 2, underscores that *the sustainability of the entire blood production chain hinges on society's voluntary and altruistic spirit of donation. Prospective blood donors are required to be treated by the principles of universality, comprehensiveness, and equity within the UnifiedHealth System (SUS)*.

This refers to the need for effective management of public organizations providing health services tocapture the donor effectively and serve the patient efficiently. In addition, public health organizations are also governed by laws and one of them is the Brazilian General Data Protection Law (LGPD), Law N.º13,709/2018 (2), which addresses the privacy of personal and sensitive data, security and availability of information to the public, not forgetting the treatment of these data. Therefore, the general objective of this article is to propose a conceptual framework using the conceptual approaches and best practices of Business Process Management (BPM) (3–10) so that a process and/or business analyst can identify vulnerable points in the organization's process that are in disagreement with the LGPD guidelines for the processing of sensitive personal data of the citizen.

This research holds significant relevance as it introduces a proposed blood donation process for the HS within an FPH with the aim of practical application of the conceptual framework put forth in this study and related works. Moreover, it's crucial to note that Business Process Management (BPM) represents a pivotal tool within the realm of Industry 4.0, extending its influence beyond traditional factory setups and physical production systems to encompass administrative processes and services (11). Another noteworthy aspect is the recent establishment of a Multidisciplinary Working Group (MWG) within the FPH, tasked with formulating overarching and specific directives to enforce the General Data Protection Law (LGPD). This endeavor involves the integration, implementation, and dissemination of a business model aligned with legal requirements across all sectors and strategic domains of the institution. This model, in turn, can serve as a blueprint for other Public and Private Hospitals housing Hemotherapy Services.

1.1 *General Data Protection Law*

The privacy of personal data has become a key security issue for various governments and companies around the world and, therefore, currently, approximately 120 countries have laws and/or regulations that aim to protect personal data that are maintained by public or private organizations (12).

One of these regulations is the General Data Protection Regulation (GDPR), which covers all residents of the European Union (EU) and applies, since May 25, 2018, to all EU Member States (13), but which was not limited to EU only, which brought consequences for many of these countries around the world, mainly in the management and sharing of health data (14–16).

The GDPR regulates and harmonizes personal data privacy laws across the EU, that is, guarantees the right of every EU citizen to control their personal data, making them their exclusive property and, making it difficult for companies to store this data without their consent (17–19). Thus, with this worldwide reach of the GDPR, Brazil sanctioned, on August 14, 2018, the General Data Protection Law (LGPD), Law 13,709 (BRAZIL, 2018), which came into force on September 18, 2020, and is based on the GDPR, the purpose of establishing the guidelines for the collection, processing, storage, and processing of personal data in Brazil (2, 12, 20, 21). In this sense, the LGPD applies to both Brazilian and foreign organizations, even those that are not physically in Brazil, but provide services that involve personal data, in order to ensure privacy, that is, the ability of each individual to control their own data (21–23).

For this control to occur, it is important that organizations take into account, in the creation of Access Control Policies (PCA) and other documents, the principles of the LGPD that guide the protection of general data, namely data quality, transparency, safety, prevention, non-discrimination and accountability (2, 22). Although these principles are fundamental so that the application of the LGPD can protect bothorganizations and people, difficulties may occur in the processing of data, especially sensitive data, that is, those involving religious conviction, political opinion, union membership, or organization of philosophical or political-religious character, referring to health or sexual, genetic or biometric life (2, 21, 24, 25). Thus, the processing of these sensitive data is in Section II - Processing of Sensitive Personal Data, arts. 11, 12, and 13 (2) is considered the main objective of the applicability of the LGPD (20). Therefore, it is up to organizations to define those responsible for the processing of sensitive personal data and for subsequent requests for personal or governmental responses involving this data (2, 21). In addition, it will be up to those responsible and their organizations to formulate PCA that suits the LGPD, seeking the implementation of privacy and security standards, technical standards, obligations for those who treat the data, educational actions for employees or servers and finally, risk supervision involving the processing of personal data, which will bring more transparency to Brazilian organizations and commitment to their users (2, 20).

1.2 *Information Security in the LGPD*

The LGPD addresses information security concepts since the recommendation of organizations to use mechanisms to ensure physical security and access to information as well as the design of the service that will be provided until its execution (2, 20). Thus, in Art. 6, item VII, is addressed one of the principles of the LGPD which is security. This principle guides the “use of technical and administrative measures that can protect personal data from unauthorized access and accidental or unlawful situations of destruction,loss, alteration, communication or dissemination” to ensure information security and data protection in general (2). Therefore, it is important that organizations have a privacy governance program that is systematically reviewed and is committed to complying with the LGPD and on the other hand, allows the user to know how the data processing is done using their information and at what point can end this processing when it is necessary (20).

There is, however, some possibility of processing users’ data without their consent, such as in compliancewith legal obligation, in the implementation of public policies created by legislation or regulation of the Federal Public Administration, for the protection of one’s own life or of third parties, by health surveillance in procedures carried out by multidisciplinary health professionals, for health services and/or for fraud prevention and security assurance of the holder in the identification and authentication processes in electronic systems (20). Thus, the application of LGPD has become a challenge and should be seen as an opportunity to redesign systems and processes capable of bringing security to the processing of personal data, especially in sensitive systems, and that collect and process many personal data (26).

2 MATERIALS AND METHOD

It was used, for the literature review, in the period from June to September 2022, the bibliographic research based, mainly, in articles of journals of the Base Scopus. Regarding the mapping of the HS business process, the BPM tool was used, which is considered an initial “driver” of work for the diagnosis and, later, for the restructuring of organizational processes, that is, a tool that can be used to diagnose and adapt the current organizational processes (phase AS-IS), in addition to the computerized systems that support these processes, the new guidelines of the legal standards established in the LGPD. Therefore, BPM serves as a tool to support the identification of parts of organizational processes (3) that present some “fragility” and require greater attention from FPH. Thus, the organization can act in the improvement and/ or reformulation of these business processes (phase TO-BE) and/ or in the improvement of their systems in order to meet the rules governing the LGPD (2) with regard to data considered personal and sensitive data.

Federal University of Rio de Janeiro
BJEDIS, Rio de Janeiro, Special Edition, v. 3 (1), 2024.
DOI: https://doi.org/10.55747/bjedis.v3i1.60729
ISSN: 2763-6925

Thus, the work proposal is divided into 3 stages and on average 4 activities per stage. A professionalwho understands the area of business processes in the organization, for example, can use the steps and activities developed from the conceptual framework to act in the identification and diagnosis of processes(phase AS-IS) that use personal and sensitive data. In this sense, the professional of the organization can act in the analysis of the process of a certain service, area, or sector of the hospital, for further improvement of this process (phase TO-BE) and processing and security of the data that are used duringthe execution of the activities and tasks for the organizational process to work. In addition, this proposal brings a conceptual approach to how personal and sensitive data can be identified in organizational processes and how to treat them, adapting them according to the legal norms of the LGPD.

The methodological design is explained in three stages, namely: 1st stage in which the mapping of the processes of the service, area, or sector of FPH occurs (Table 1); 2nd stage in which there is the diagnosis of these processes (Table 2) and the 3rd stage in which the adequacy of the processes to LGPD occurs (Table 3). Thus, below is briefly described how a solution was proposed to identify in the business processes of the organization the points of non-compliance with the LGPD. The 1st Stage, Process Mapping (phase AS-IS), focuses on the identification of personal data and is divided into 3 activities described in Table 1.

Table 1. Process Mapping in the 1st Stage

Activity	Description
1	Perform the mapping of the processes of the service, area, or sector of the hospital using the good practices of BPM.
2	Identify and point out in the processes which are the personal and sensitive data in each task and/ or activity that use this data, regardless of whether they are manual or systemic tasks.
3	Carry out the inventory of personal and sensitive data or create an initial (unrefined) data matrix with the identified data, classifying it as personal data and sensitive data.

In Stage 2, the diagnosis is made (phase AS-IS) and is divided into 5 activities described in Table 2.

Table 2. Diagnosis (AS-IS phase) in the 2nd Stage

Activity	Description
1	Identify in the mapped processes the tasks and/or activities that use personal and sensitive data.
2	Identify in the processes who are the main actors responsible for maintaining and usingthis data.
3	Identify in the mapped processes how these data enter the process, how they are organized, how and how they are manipulated, where and by what means, (for example spreadsheets, systems, email, digitization, and others) these data are processed in the processes and how they are discarded.
4	Identify which are the systems that offer vulnerability to the processes of the service, area, or sector of the hospital and where there is the crossing (borders of the processes) of data with the other services, areas, or sectors, in addition to the exchanges of data between systems, pointing out in the mapped processes (even if they are outside the scope of the current analysis), which data and systems cross the borders of other services, areas or sectors that use the same data. Thus, when this work approach is used in other services, areas or sectors of the hospital will already facilitate the initial diagnosis

	of the process (phase AS-IS) to be analyzed.
5	Refine the inventory sheet of personal and sensitive data or the initial data matrix of the previous step with the identified data, classifying them as personal data and sensitive data.

In Stage 3, the adequacy of organizational processes to the LGPD (phase TO-BE) is treated and isdivided into 5 activities described in Table 3.

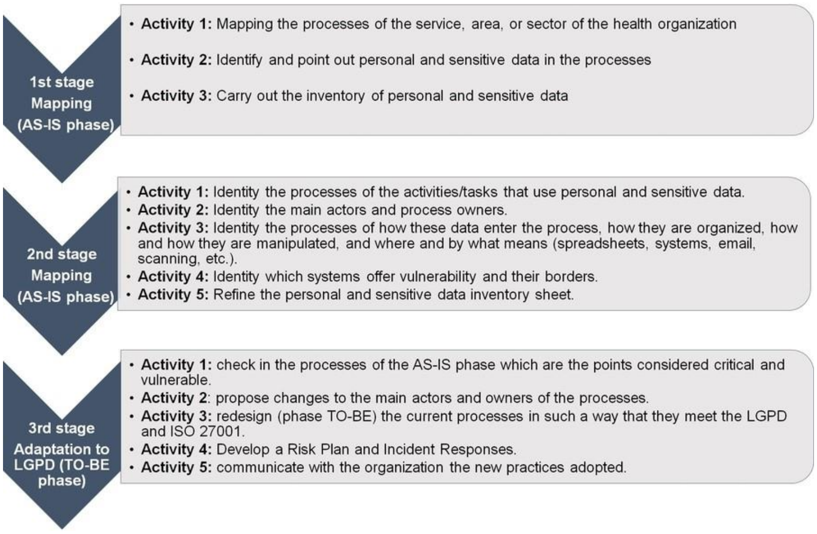
Table 3. The alignment of organizational processes with LGPD (phase TO-BE) in Stage 3

Activity	Description
1	Verify in the processes of the AS-IS phase which are the points considered critical and vulnerable that are exposing personal data and/or sensitive data.
2	Propose changes to the main actors and owners of the processes of the service, area, or sector of the hospital organization.
3	Redesign (phase TO-BE) the current processes in such a way that meet the legal compliance of the LGPD. These changes should also be thought of with a focus on adapting to ISO 27001 which addresses Information Security in the context of the organization.
4	Elaborate on the Risk Plan and Incident Responses, in case of leakage or Cyberattacks on personal data. In this case, the organization can adopt the practices and adapt them to the Safety Incident Response Guide, prepared by the Ministry of Planning.
5	Communicate the practices adopted to mitigate the risks of information leakage.

Finally, Fig. 1 summarizes a proposal for a conceptual framework of the organizational process (service, area, or FPH sector) to be analyzed to adapt them to the legal norms of the LGPD.

Federal University of Rio de Janeiro
BJEDIS, Rio de Janeiro, Special Edition, v. 3 (1), 2024.
DOI: https://doi.org/10.55747/bjedis.v3i1.60729
ISSN: 2763-6925

Figure 1. Proposal for a conceptual framework to meet LGPD standards using BPM



1st stage Mapping (AS-IS phase)

- **Activity 1:** Mapping the processes of the service, area, or sector of the health organization
- **Activity 2:** Identify and point out personal and sensitive data in the processes
- **Activity 3:** Carry out the inventory of personal and sensitive data

2nd stage Mapping (AS-IS phase)

- **Activity 1:** Identity the processes of the activities/tasks that use personal and sensitive data.
- **Activity 2:** Identity the main actors and process owners.
- **Activity 3:** Identity the processes of how these data enter the process, how they are organized, how and how they are manipulated, and where and by what means (spreadsheets, systems, email, scanning, etc.).
- **Activity 4:** Identity which systems offer vulnerability and their borders.
- **Activity 5:** Refine the personal and sensitive data inventory sheet.

3rd stage Adaptation to LGPD (TO-BE phase)

- **Activity 1:** check in the processes of the AS-IS phase which are the points considered critical and vulnerable.
- **Activity 2**: propose changes to the main actors and owners of the processes.
- **Activity 3:** redesign (phase TO-BE) the current processes in such a way that they meet the LGPD and ISO 27001.
- **Activity 4:** Develop a Risk Plan and Incident Responses.
- **Activity 5:** communicate with the organization the new practices adopted.

Therefore, it is through these three stages and the activities that make up each stage that a model is proposed that can treat personal and sensitive data, in addition to information security, using BPM as asupport tool and at the same time, to meet the legal requirements imposed by the LGPD.

3 RESULTS AND DISCUSSION

In 2021, the HS of FPH performed approximately 14,569 transfused hemocomponents, which produced 9063 red blood cell concentrates, 8662 random platelet concentrates of 5 days, 8748 fresh plasma, 764 platelet concentrates per apheresis, 10 lymphocyte concentrates, 18 granulocyte concentrates and 72 hematopoietic progenitor cells, operating seven days a week, twenty-four hours a day. In addition, 12,014 screenings/year, captured 12,000 possible donors/year and performed 10,075 collections/year. With this demand and complexity, the interruption or failure at some point in the SSC process can lead to several problems in the treatment of patients who are treated in the HS of FPH and the capture of donors for the maintenance of their stock of blood bags.

Regarding the process, it begins when a candidate for blood donation arrives at the reception and receives a password (numbered plastic card) for arrival control. Then the candidate is called by the password and served in the reception sector. This service at the reception consists of registering the candidate for donation in the computerized system, hereinafter called the Hemotherapy Management System (SGH) of the HS, where the personal data of the candidate and the information on the type of donation are recorded. Thus, after the registration of the candidate, this register is now viewed in the service queue of the SGH of the clinical triage area, waiting at the reception to be called to one of the offices of the clinical triage sector. The employee of this sector (called "triador") calls verbally at the reception of the HS the candidate to be evaluated (weight, pressure, height, pulse, and hemoglobin) and then he is interviewed.

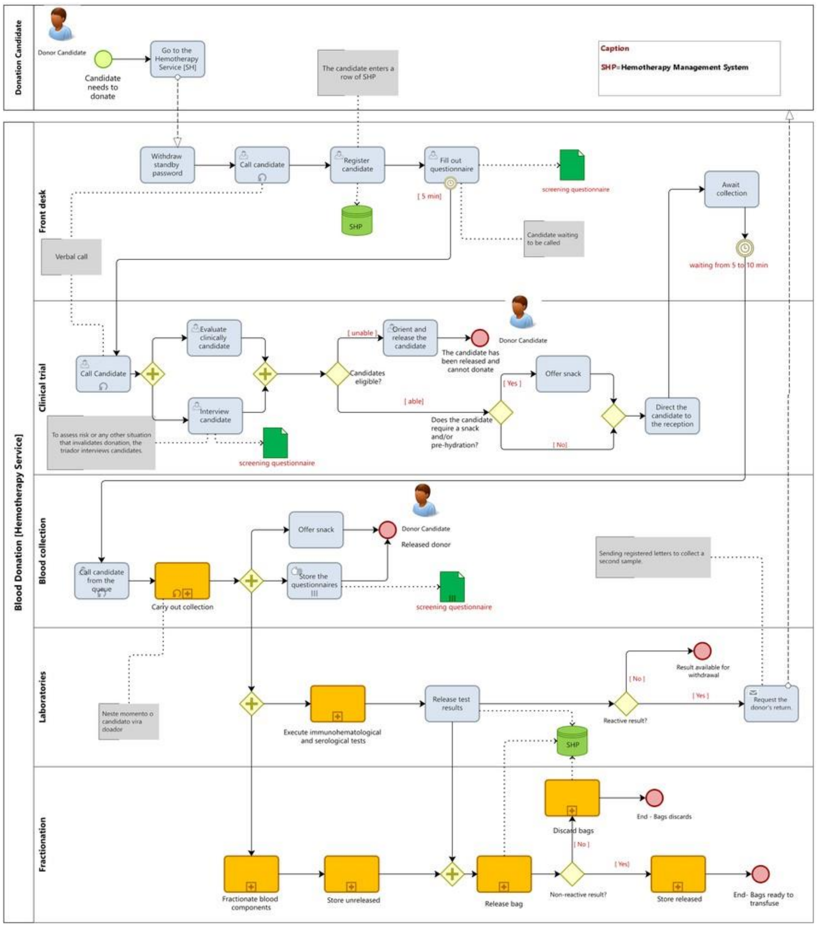
After the interview, if necessary, the "triador" sends the candidate to snack. However, if the candidate can triage, it will be viewed in the SGH service queue to perform blood collection. However, if he is unfit, the candidate is guided and released from the donation. Soon after, the candidate fit for the donation awaits to be called at the reception by the blood donation collection department, which occurs after a few minutes when the employee of this sector views the candidates in the SGH and calls the next candidate of the queue for attendance.

Thus, at the end of the blood collection, there is the completion of the form (screening questionnaire) by the employee who collected the donation data (beginning, end, total time, number of bag segments, number of homogenizers used, number of collectors, volume collected and if there were complications). Finally, the employee of this area sees if the donor is okay and if so, directs him to have a snack, releasing him then.

In the sequence, the employee of the blood collection area places the bag in a plastic tray containing the blood bag and blood tubes collected. Then the laboratory staff collects the tubes containing the blood for immunohematology and serology tests, as well as the employees of the fractionation area collect the tubes to perform fractionations of blood products and subsequent release of blood bags to be transfused. When the fractionation area arrives and if the result of the blood test is reactive, that is, after the tests, it turns out that some of the components are unsuitable for donation, the bag is discarded. In the laboratory area, if any non-conformity is found in the results of immunohematological and/or serological tests (reactive result), the donor is communicated by a registered letter to perform a second test/collection. Therefore, for a better understanding of the blood donation business process, the modeling of this process (phase AS-IS) performed in the HS of the FPH is presented in Figure 2.

Federal University of Rio de Janeiro
BJEDIS, Rio de Janeiro, Special Edition, v. 3 (1), 2024.
DOI: https://doi.org/10.55747/bjedis.v3i1.60729
ISSN: 2763-6925

Figure 2. Blood donation process approaching the AS-IS phase of a Hemotherapy Service of an FPH.


Donation Candidate
Donor Candidate
Candidate needs to donate
Go to the Hemotherapy Service [SH]
The candidate enters a row of SHP
Caption
SHP=Hemotherapy Management System
Blood Donation [Hemotherapy Service]
Front desk
Withdraw standby password
Call candidate
Register candidate
Fill out questionnaire
screening questionnaire
[5 min]
SHP
Candidate waiting to be called
Verbal call
Await collection
waiting from 5 to 10 min
Clinical trial
Call Candidate
Evaluate clinically candidate
Interview candidate
To assess risk or any other situation that invalidates donation, the triador interviews candidates.
screening questionnaire
Candidates eligible?
[unable]
[able]
Orient and release the candidate
The candidate has been released and cannot donate
Donor Candidate
Does the candidate require a snack and/or pre-hydration?
[Yes]
[No]
Offer snack
Direct the candidate to the reception
Blood collection
Call candidate from the queue
Carry out collection
Offer snack
Store the questionnaires
Donor Candidate
Released donor
screening questionnaire
Sending registered letters to collect a second sample.
Laboratories
Neste momento o candidato vira doador
Execute immunohematological and serological tests
Release test results
SHP
Reactive result?
[No]
[Yes]
Result available for withdrawal
Request the donor's return.
Fractionation
Fractionate blood components
Store unreleased
Release bag
Discard bags
End - Bags discards
Non-reactive result?
[No]
[Yes]
Store released
End- Bags ready to transfuse

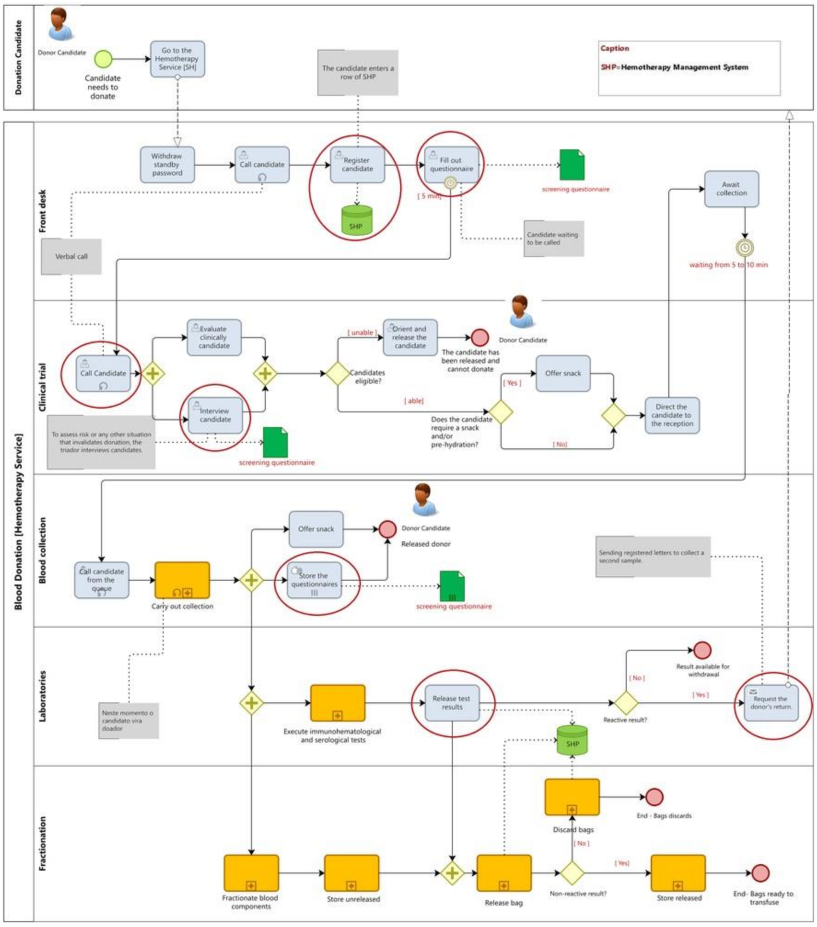
There are sub processes that were not modeled in this work, as it would make the model more complex . Through the mapping of the HS process (Figure 2) the points of vulnerabilities of the data, considered personal and sensitive, of the candidate for blood donation or the routine donor, are evident. Among these points of vulnerability is the form (screening questionnaire) on paper, which circulates between areas ofthe HS of the FPH. In the mapping carried out, the donation candidate himself takes the completed formfrom the reception waiting area to the clinical screening area so that the information is complemented byan employee who collects the blood. In addition, the security of donor and donor information may be compromised, because there is a need to survey the levels and types of access that are allowed to users during the service process and what types of data are available and do not hurt the LGPD.

Thus, Figure 2 was marked by circles with the points of attention in the blood donation process in which vulnerabilities were found and that must be corrected to adapt the donation process from the HS to the LGPD. In this way, at these points of the process marked, you can act, align and redefine (redesign)the process (phase TO-BE) to meet the minimum requirements or the entire. It is expected that this way the new process is adequate and adjusted to the current rules of the Law. It is essential that the activities proposed in the conceptual framework are documented, and that the artifacts (datasheet, risk plan, and responses to incidents) are in operation. In addition, to ensure security throughout the process,users and actors responsible for the processes, as well as the HPF, know how to act in the event of leakage of personal and sensitive data or any type of information that may compromise the identification of the donor candidate, who is donating, the doctor or even anyone related to the process. Therefore, for FPH processes

Federal University of Rio de Janeiro
BJEDIS, Rio de Janeiro, Special Edition, v. 3 (1), 2024.
DOI: https://doi.org/10.55747/bjedis.v3i1.60729
ISSN: 2763-6925

to be aligned with LGPD (2), there is a need for continuous training of all those involved in the pillars of the LGPD that deals with the protection of personal and sensitive data; define what limits andscope the LGPD acts on these organizational processes to understand what data (from the donor, the doctor or even a collaborator) can be disclosed, to whom and in what way; how they should circulate in the services of a public hospital or, between other services of the organization or even among other public hospitals; the alignment of all services of the public organization as: what types of data are sensitive or not; what types and forms the citizen's data (donors or patients) can be disclosed; how and what incidents, if any, should be reported to the National Data Protection Agency (ANPD) (27) to comply with the new regulations of the LGPD, as outlined in Figure 3.

Figure 3. Points of attention (vulnerabilities) of the blood donation process addressed in the AS-IS phase.


Donation Candidate
Donor Candidate
Candidate needs to donate
Go to the Hemotherapy Service [SH]
The candidate enters a row of SHP
Caption
SHP=Hemotherapy Management System
Blood Donation [Hemotherapy Service]
Front desk
Withdraw standby password
Call candidate
Register candidate
SHP
Fill out questionnaire
[5 min]
screening questionnaire
Candidate waiting to be called
Verbal call
Await collection
waiting from 5 to 10 min
Clinical trial
Call Candidate
Evaluate clinically candidate
Interview candidate
To assess risk or any other situation that invalidates donation, the triador interviews candidates.
screening questionnaire
Candidates eligible?
[unable]
Orient and release the candidate
The candidate has been released and cannot donate
Donor Candidate
[able]
Does the candidate require a snack and/or pre-hydration?
[Yes]
Offer snack
[No]
Direct the candidate to the reception
Blood collection
Call candidate from the queue
Carry out collection
Offer snack
Donor Candidate
Released donor
Store the questionnaires
screening questionnaire
Sending registered letters to collect a second sample.
Laboratories
Neste momento o candidato vira doador
Execute immunohematological and serological tests
Release test results
Reactive result?
[No]
Result available for withdrawal
[Yes]
Request the donor's return.
SHP
Fractionation
Fractionate blood components
Store unreleased
Release bag
Non-reactive result?
[No]
Discard bags
End - Bags discards
[Yes]
Store released
End- Bags ready to transfuse

As recommended by activity 3 (Figure 1) of the proposed conceptual framework, there is a need for professionals of HS administration and the direction of FPH to reevaluate the AS-IS process with the main actors that interact with the organizational process. The communication should be part of the routine of the organization after the remodeling of the process, considering that the HS will already be aligned with the new guidelines of the LGPD making the process more effective, and efficient and therefore insurance for both the donation candidates and blood donors and the respective employees of the organization who work in the HS process.

Federal University of Rio de Janeiro
BJEDIS, Rio de Janeiro, Special Edition, v. 3 (1), 2024.
DOI: https://doi.org/10.55747/bjedis.v3i1.60729
ISSN: 2763-6925

CONCLUSION

This work brought the proposal of a conceptual framework to be applied in the organizational processes of public and private hospitals, using the best practices of BPM, which facilitates the identification of vulnerable points that can lead to leakage of data people from possible blood donors. In addition, it discusses how processes can be corrected and appropriate to meet the current standards in the new LGPD(2).

Using the activities of the conceptual framework, the modeling of the blood donation process (phase AS-IS) of the HS of an FPH, in Rio de Janeiro, Brazil, was performed. Thus, the results found in the mapped process show that personal data considered sensitive by the LGPD are vulnerable, enabling the leakage of information that can compromise the CSS security process.

This work did not address the restructuring and redesign of the process (TO-BE phase) (5, 7) of blooddonation of the HS, which corresponds to the third stage of the conceptual framework, which process is in the review phase by the main actors of the organization. In addition, the Risk and Incidents plan (28) isbeing prepared by the MWG that operates in the implementation of the GDPL.

CONFLICT OF INTEREST

There is no conflict of interest.

ACKNOWLEDGEMENTS

The authors of this work thank the Hemotherapy Service of the National Cancer Institute (INCA).

Author statement

Emmanuel Pires: Conceptualization, Methodology, Data analysis, and Writing-Original draft preparation. Claudio Luiz de Oliveira Costa: Conceptualization, Igor Leão dos Santos: Conceptualization, Supervision and Reviewing. Augusto da Cunha Reis: Reviewing. Keicia Pinto: Data analysis

References

1 BRASIL. Ministério da Saúde. PORTARIA N.º 158, DE 4 DE FEVEREIRO DE 2016.
Redefine o regulamento técnico de procedimentos hemoterápicos. 2016. Available from: https:
//bvsms.saude.gov.br/bvs/saudelegis/gm/2016/prt0158_04_02_2016.html.

2 BRASIL. Presidência da República. Secretaria-Geral Subchefia para Assuntos Jurídicos. LEI N.º 13.709. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD). Diário Oficial da União. 2018.
Available from: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

3 Dumas M, Rosa ML, Mendling J, Reijers HA. In: Dumas M, Rosa ML, Mendling J, Reijers HA, editors. Process Identification. Berlin, Heidelberg: Springer Berlin Heidelberg; 2018. p. 35 73. Availablefrom: https://doi.org/10.1007/978-3-662-56509-4_2.

4 Dumas M, Rosa ML, Mendling J, Reijers HA. In: Dumas M, Rosa ML, Mendling J, Reijers HA, editors. Essential Process Modeling. Berlin, Heidelberg: Springer Berlin Heidelberg; 2018. p. 75 115. Available from: https://doi.org/10.1007/978-3-662-56509-4_3.

5 Dumas M, Rosa ML, Mendling J, Reijers HA. In: Dumas M, Rosa ML, Mendling J, Reijers HA, editors. Advanced Process Modeling. Berlin, Heidelberg: Springer Berlin Heidelberg; 2018. p.

117 157. Available from: https://doi.org/10.1007/978-3-662-56509-4_4.

6 Dumas M, Rosa ML, Mendling J, Reijers HA. In: Dumas M, Rosa ML, Mendling J, Reijers HA, editors. Process Discovery. Berlin, Heidelberg: Springer Berlin Heidelberg; 2018. p. 159 212. Available from: https://doi.org/10.1007/978-3-662-56509-4_5.

7 Dumas M, Rosa ML, Mendling J, Reijers HA. In: Dumas M, Rosa ML, Mendling J, Reijers HA, editors. Process Redesign. Berlin, Heidelberg: Springer Berlin Heidelberg; 2018. p. 297 339. Available from: https://doi.org/10.1007/978-3-662-56509-4_8.

8 Dumas M, Rosa ML, Mendling J, Reijers HA. In: Dumas M, Rosa ML, Mendling J, Reijers HA, editors. Qualitative Process Analysis. Berlin, Heidelberg: Springer Berlin Heidelberg; 2018. p. 213 254. Available from: https://doi.org/10.1007/978-3-662-56509-4_6.

9 Dumas M, Rosa ML, Mendling J, Reijers HA. In: Dumas M, Rosa ML, Mendling J, Reijers HA, editors. Essential Process Modeling. Berlin, Heidelberg: Springer Berlin Heidelberg; 2018. p. 75 115. Available from: https://doi.org/10.1007/978-3-662-56509-4_3.

10 Dumas M, RosA ML, Mendling J, Reijers HA. In: Dumas M, RosA ML, Mendling J, Reijers HA, editors. Quantitative Process Analysis. Berlin, Heidelberg: Springer Berlin Heidelberg; 2018. p. 255 296. Available from: https://doi.org/10.1007/978-3-662-56509-4_7.

11 Turra MED, Juliani LI, da Costa Gonçalves Salla NM. Gestão de Processos de Negócio – BPM: Um Estudo Bibliométrico sobre a Produção Científica Nacional. Revista Administração em Diálogo - RAD. 2018 Setembro;20(3):46 68. Available from: https://revistas.pucsp.br/index.php/rad/article/ view/36961.

12 Silva J, Calegari N, Gomes E. After Brazil's General Data Protection Law: Authorization in Decentralized Web Applications. In: Companion Proceedings of The 2019 World Wide Web Conference.WWW '19. New York, NY, USA: Association for Computing Machinery; 2019. p. 819 822. Available from: https://doi.org/10.1145/3308560.3316461.

13 Todde M, Beltrame M, Marceglia S, Spagno C. Methodology and workflow to perform the Data Protection Impact Assessment in healthcare information systems. Informatics in Medicine Unlocked. 2020;19. Available from: https://www.sciencedirect.com/science/article/pii/S2352914820301477.

14 Crozier-Shaw G, Hughes AJ, Cashman J, Synnott K. Instant messaging apps and data protection: combining to improve hip fracture care? Irish journal of medical science. 2021 4;191:765 769. Availablefrom: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8020372/.

15 Shabani M, Borry P. Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. European journal of human genetics : EJHG. 2017 12;26:149 156. Available from: https://doi.org/10.1038/s41431-017-0045-7.

16 Yuan B, Li J. The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation. International journal of environmental research and public health. 2019 4;16. Available from: https://doi.org/10.3390/ijerph16061070.

17 Georgiou D, Lambrinoudakis C. Data Protection Impact Assessment (DPIA) for Cloud-Based Health Organizations. Future Internet. 2021;13(3). Available from: https://www.mdpi.com/1999-5903/13/ 3/66.

18 Nomura S, Sakamoto H, Ishizuka A, Katsuma Y, Akashi H, Miyata H. Ongoing debate on data governance principles for achieving Universal Health Coverage: a proposal to post-G20 Osaka Summit meetings. Global Health Action. 2020;13(1). PMID: 33334272. Available from: https://doi.org/ 10.1080/16549716.2020.1859822.

19 Watts P, Breedon P, Nduka C, Neville C, Venables V, Clarke S. Cloud Computing Mobile Application for Remote Monitoring of Bell's Palsy. Journal of medical systems. 2020 7;44:149. Available from: https://link.springer.com/article/10.1007/s10916-020-01605-7.

20 Ferrão SER, Carvalho AP, Canedo ED, Mota APB, Costa PHT, Cerqueira AJ. Diagnostic of Data Processing by Brazilian Organizations—A Low Compliance Issue. Information. 2021;12(4). Available from: https://www.mdpi.com/2078-2489/12/4/168.

21 Piurcosky FP, Calegário C, Costa M, Frogeri RF. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. Suma de Negocios. 2019 Jul-Dez;10(23):89 99. Available from: http://dx.doi.org/10.14349/sumneg/2019.V10.N23.A2.

22 Canedo ED, Calazans ATS, Cerqueira AJ, Costa PHT, Masson ETS. Agile Teams' Perception in Privacy Requirements Elicitation: LGPD's compliance in Brazil. In: 2021 IEEE 29th International Requirements Engineering Conference (RE); 2021. p. 58 69. Available from: https:
//ieeexplore.ieee.org/document/9604706.

23 Kalloniatis C, Kavakli E, Gritzalis S. Addressing privacy requirements in system design: the PriS method. Requirements Eng. 2008;13:241 255. Available from: https://www.icsd.aegean.gr/ publication_files/609984034.pdf.

24 GIARLLARIELLI ADVOGADOS. Guia LGPD; 2022. Available from: https://www.giarllarielli.adv.br/guia-lgpd/.

25 UE. Parlamento Europeu do Conselho. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU DO CONSELHO. Jornal Oficial da União Europeia. 27 de abril de 2016. Available from: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679.

26 Diamantopoulou V, Androutsopoulou A, Gritzalis S, Charalabidis Y. Preserving Digital Privacy in e-Participation Environments: Towards GDPR Compliance. Information. 2020;11(2). Available from: https://www.mdpi.com/2078-2489/11/2/117.

Federal University of Rio de Janeiro
BJEDIS, Rio de Janeiro, Special Edition, v. 3 (1), 2024.
DOI: https://doi.org/10.55747/bjedis.v3i1.60729
ISSN: 2763-6925

27 BRASIL Autoridade Nacional de Proteção de Dados (ANPD). Comunicação de incidente de segurança; 2023. Available from: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis.

28 BRASIL Ministério da Saúde Departamento de Atenção Especializada e Temática (DAET). Plano de Atenção para o Diagnóstico e o Tratamento do Câncer; 2023. Available from: https://www.gov.br/ saude/pt-br/composicao/saes/daet.