A Privacy Threat Modeling Method for Healthcare Systems under the Brazilian LGPD

Giovana N. Oliveira[1], Isabelle C. P. S. Costa[2], Ricardo G. Aguiar[3], Rodrigo M. Pagliares[1]

[1]Department of Computer Science – Universidade Federal de Alfenas (UNIFAL)
Alfenas – MG – Brazil

[2]Nursing School – Universidade Federal de Alfenas (UNIFAL)
Alfenas – MG – Brazil

[3]Institute of Motricity Sciences – Universidade Federal de Alfenas (UNIFAL)
Alfenas – MG – Brazil

giovana.nogueira@sou.unifal-mg.edu.br,
{isabelle.costa, ricardo.aguiar, rodrigo.pagliares}@unifal-mg.edu.br

Abstract. *The digitalization of healthcare increases privacy risks associated with sensitive data processing. Although the Brazilian General Data Protection Law (LGPD) mandates data protection, healthcare organizations often focus on generic security controls and lack structured privacy engineering to address threats such as linkability and identifiability. This paper proposes a privacy threat modeling method for healthcare systems under the LGPD. The method was evaluated through a case study involving the Nursing Process Application System (SisAPEC), a system deployed within the Brazilian Unified Health System (SUS). The method includes system modeling and systematic threat elicitation steps, which in the case study were implemented using Data Flow Diagrams and the LINDDUN framework. The application of the method identified 14 privacy threats, which were mapped to Privacy-Enhancing Requirements (PERs), establishing traceability between regulatory and technical requirements. The results indicate that the method operationalizes Privacy by Design by establishing traceability between legal requirements and architectural privacy requirements.*

1. Introduction

The digitalization of healthcare through Electronic Health Records (EHR) and telehealth improves clinical efficiency but increases risks to sensitive personal data [Obaid and Salman 2022]. In Brazil, the General Data Protection Law (LGPD) governs this processing, establishing principles such as purpose limitation, necessity, and transparency that apply throughout the data lifecycle [Brasil 2018].

Despite this regulatory framework, healthcare organizations often focus on basic security measures that do not address privacy as an independent concern [Sahi et al. 2017, Aijaz et al. 2023]. Traditional security frameworks are often not designed to capture specific privacy risks, such as data linkability and detectability [Azam et al. 2023]. Consequently, technical teams face challenges in translating legal principles into concrete system requirements during development [Severo et al. 2025].

This paper proposes a privacy threat modeling method under the LGPD, providing a workflow to identify threats in Brazilian Unified Health System (SUS) core processes

and map them to Privacy-Enhancing Requirements (PERs). The method was evaluated via a case study of the Nursing Process Application System (SisAPEC), an EHR system used in the SUS. The subsequent sections describe the background, the method, its application, and results regarding technical-legal traceability.

2. Background

The LGPD classifies health data as sensitive, requiring legal bases like health tutelage for processing. Beyond defining roles (Controller, Operator, Data Protection Officer (DPO)), compliance depends on translating regulatory principles into verifiable architectural constraints [Corrêa and Franco 2025, Semantha et al. 2020], a bridge for system characterization under data protection laws [Quincozes et al. 2023]. Privacy by Design (PbD) addresses this by integrating safeguards into architecture and data flows from the initial stages as a default functional property [Gürses et al. 2011, Cavoukian 2009].

Privacy threat modeling is an engineering approach to identify and mitigate privacy risks throughout the software lifecycle. In this scope, Data Flow Diagrams (DFDs) are used to represent architecture through processes, data flows, and trust boundaries [Sion et al. 2018]. Upon these DFDs, the LINDDUN framework [Wuyts et al. 2020] is applied to elicit threats across seven categories: Linkability, Identifiability, Non-repudiation, Detectability, Information Disclosure, Unawareness, and Non-compliance. This taxonomy addresses specific privacy risks, such as data linkage, which traditional security frameworks often overlook [Deng et al. 2011].

The SUS processes sensitive personal data across a decentralized network [Paim et al. 2011]. Within this context, SisAPEC is an AI-powered tool used in primary care and hospitals to support clinical reasoning and nursing diagnoses via Large Language Models (LLMs).

3. The Proposed Method

The proposed method (Figure 1) is an input-process-output workflow designed to align privacy engineering with LGPD requirements. It comprises six steps where a Privacy Engineer (PE) and a DPO collaborate to establish technical-legal traceability through the consumption and production of artifacts. To demonstrate feasibility, the method's application to SisAPEC is presented alongside each step. This case study is limited to architectural and process modeling, excluding the processing of real personal data from patients or healthcare professionals.

In the first step, the PE utilizes system documentation to identify assets, defined as any physical, logical, or informational component of value to the organization or the data subject [OWASP Foundation 2026]. Assets are grouped into technical and logical domains to establish the technical scope (Asset Inventory). Applied to SisAPEC, this process resulted in an inventory spanning three domains (Table 1), representing the system's informational core. In the second step, the DPO classifies these assets based on LGPD Art. 5, producing the Data Sensitivity Classification. For SisAPEC, workstation and infrastructure assets (A1, A2) were classified as Personal Data, while clinical reasoning assets (A3.3) were classified as Sensitive Personal Data.

In the third step, the PE integrates the previous artifacts into DFDs to map information movement and establish the technical foundation for threat elicitation

[OWASP Foundation 2026]. By identifying trust boundaries and transitions in data control, the DFD serves as the primary analysis unit. For SisAPEC, this resulted in a Level 1 DFD (Figure 2) that decomposes the architecture into seven core processes (P1–P7) and six data stores (DS1–DS6), capturing the data lifecycle from authentication to clinical reasoning.

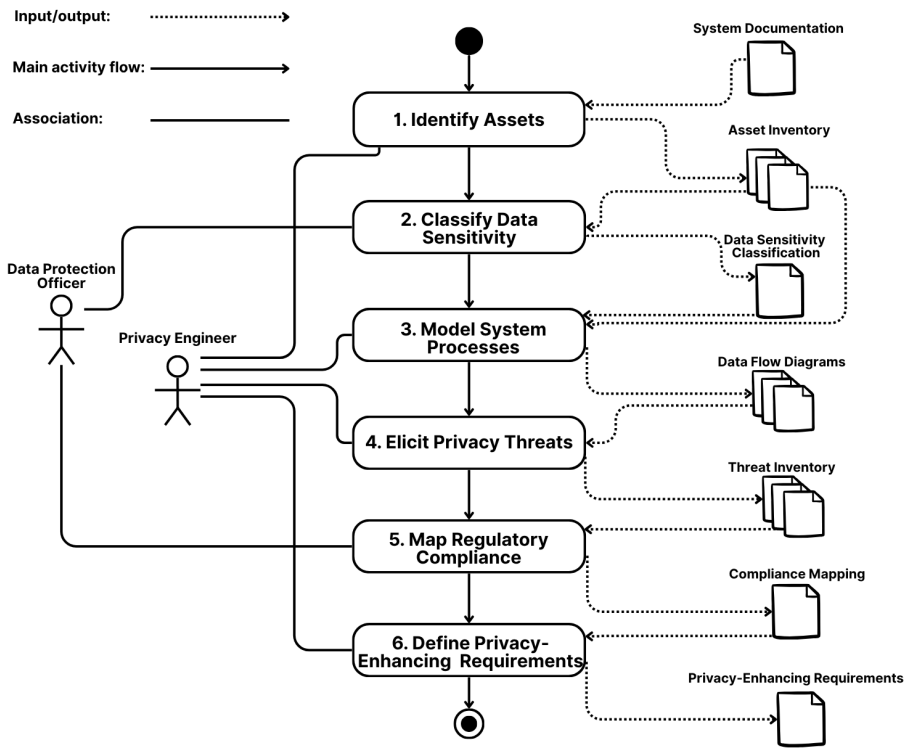

Figure 1. Workflow of the proposed method

Table 1. Technical asset inventory and data sensitivity classification (Steps 1-2)

Asset ID	Asset Name / Component	System Domain	LGPD Category
A1	User Credentials and Sessions	Workstation	Personal Data
A2	API and System Logs (IPs, IDs)	Infrastructure	Personal Data
A3.1	Professional and Clinic Data	Data Assets	Personal Data
A3.2	Patient Identifiers (Name, Address)	Data Assets	Personal Data
A3.3	Patient Health Data (Anamnesis)	Data Assets	Sensitive Personal Data

In the fourth step, the PE identifies privacy threats by applying a structured taxonomy to the DFD. By mapping each process, the data lifecycle is analyzed to produce a Threat Inventory. In the SisAPEC case study, the LINDDUN framework [Wuyts et al. 2020] was applied, identifying fourteen privacy threats. Table 2 illustrates representative examples of these threats and their impacted assets.

In the fifth step, the DPO connects technical threats to the LGPD, identifying compromised principles to produce the Compliance Mapping. For instance, Linkability and Identifiability threats were mapped to the principle of Necessity (Art. 6, III), as using persistent identifiers—such as the Individual Taxpayer Registry (CPF)—without

pseudonymization exceeds the minimum data required for clinical purposes, providing the regulatory justification for subsequent requirements.

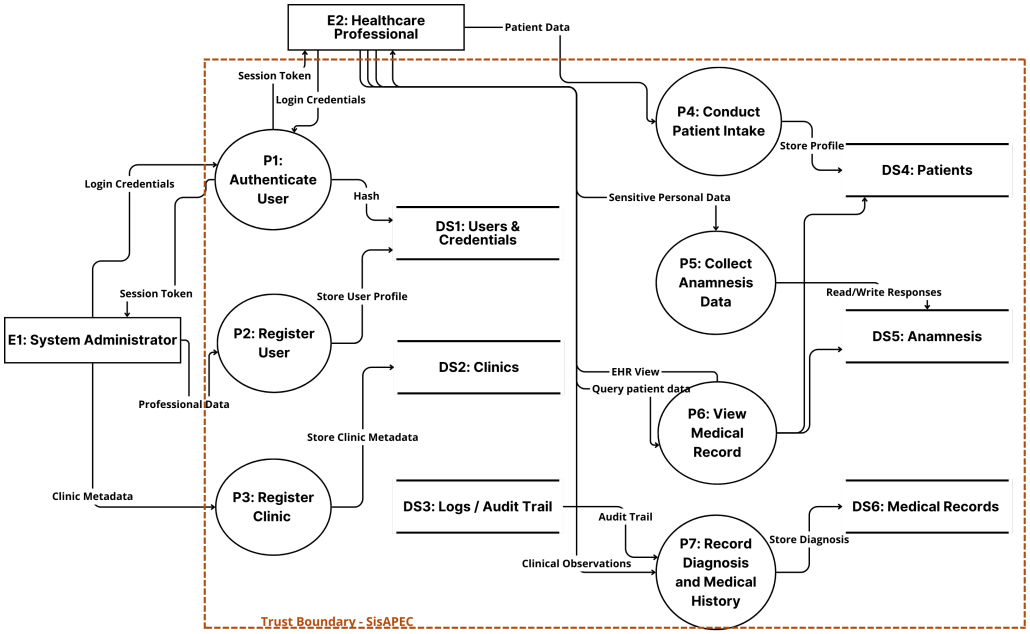

Figure 2. Level 1 Data Flow Diagram (DFD) of the SisAPEC healthcare system

In the final step, the PE translates the Compliance Mapping into PERs, which function as high-level architectural or procedural constraints to reduce privacy risks [Hoepman 2014]. These requirements transform legal obligations into concrete constraints for developers. Applied to SisAPEC, this resulted in seven PERs; Table 3 presents a subset of these requirements mapped to their respective LGPD bases. For instance, non-repudiation threats (NrT1, NrT2) led to requirements for immutable digital audit trails to satisfy accountability (Art. 6, X).

Table 2. Privacy threat inventory for SisAPEC (Step 4)

ID	Threat Name	Description / Summary	Assets
NrT1	Repudiation of Access	Inability to prove access due to lack of signed logs.	A2
NrT2	Repudiation of Creation	Inability to verify the origin of clinical entries.	A3.3
NcT2	Subject Rights	Missing interfaces for portability and correction.	A3.2, A3.3

Table 3. Mapping of threats to LGPD bases and PERs (Steps 5-6)

Threat IDs	LGPD Basis	Privacy-Enhancing Requirements
NrT1, NrT2	Art. 6, X (Accountability); Art. 37	Immutable Digital Audit Trails
NcT2	Art. 18 (Subject Rights)	Data Subject Rights Dashboard

4. Results and Discussions

The application of the method to the SisAPEC system identified 14 privacy threats. While Tables 2 and 3 show selected examples, the complete analysis suggests that the workflow

is framework-independent, allowing the integration of alternatives like STRIDE-Privacy or the risk-centric PASTA adapted for data protection requirements [Azam et al. 2023].

By transforming legal principles into PERs, the method bridges the gap between privacy and regulatory compliance. In SisAPEC, linkability and identifiability threats originate from the reliance on persistent identifiers (e.g., CPF, CNS), which facilitate clinical care but enable unauthorized correlation across repositories. To mitigate this, PERs for detectability employ traffic obfuscation to address metadata-level risks that encryption alone cannot resolve, fulfilling the prevention principle (LGPD Art. 6, VIII).

This method operationalizes PbD and accountability (Art. 6, X) by prioritizing technical artifacts over generic policy checklists, revealing threats like presence inference, often missed in conventional audits. These high-level PERs serve as architectural constraints to be decomposed into technical tasks via, for instance, a Requirements Breakdown Structure (RBS) [Faulconbridge and Ryan 2018]. Furthermore, although evaluated in healthcare, the workflow is adaptable to other regulated domains where technical-legal traceability is required, though further cross-domain validation is necessary.

5. Conclusion

This paper proposed an LGPD-aligned privacy threat modeling method using DFDs and LINDDUN, evaluated via the SisAPEC system. The analysis identified 14 threats in core nursing processes mapped to PERs. Results indicate that the proposed method operationalizes PbD by establishing traceability between regulatory and architectural requirements, identifying specific LGPD-related threats and privacy flaws in the system's design.

6. Future Work

Future work involves the possibility of external validation through method replication by independent teams to assess result consistency. Comparative studies between LINDDUN and alternative taxonomies could characterize the impact of different methodologies on threat elicitation. Additionally, the development of a RBS to quantify implementation effort and cost remains an opportunity for investigation. Finally, validation in other regulated sectors is a potential step to evaluate cross-domain applicability.

Acknowledgments

This research was supported by the National Council for Scientific and Technological Development (CNPq) under grant 444704/2024-8 (ConhecBrasil-REDES) and by the Fundação de Amparo à Pesquisa do Estado de Minas Gerais (FAPEMIG) under grant APQ-04855-23. This study was also financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001. Institutional support was provided by the Universidade Federal de Alfenas (UNIFAL-MG).

References

Aijaz, M. et al. (2023). Threat modeling and assessment methods in the healthcare-it system: A critical review and systematic evaluation. *SN Computer Science*, 4.

Azam, N. et al. (2023). Data privacy threat modelling for autonomous systems: A survey from the gdpr's perspective. *IEEE Transactions on Big Data*, 9(2):388–414.

Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Presidência da República. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed: November 25, 2024.

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Technical report, Information and Privacy Commissioner of Ontario.

Corrêa, H. and Franco, M. F. (2025). Lei geral de proteção de dados (lgpd) na saúde: Tendências, desafios e oportunidades. In *Anais da XXII Escola Regional de Redes de Computadores (ERRC)*, pages 123–129. SBC.

Deng, M., Wuyts, K., Scandariato, R., Preneel, B., and Joosen, W. (2011). A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*, 16:3–32.

Faulconbridge, R. I. and Ryan, M. J. (2018). *Systems Engineering Practice*. Argos Press.

Gürses, S., Troncoso, C., and Diaz, C. (2011). Engineering privacy by design. In *Conference on Computing and Communication Workshop*.

Hoepman, G. (2014). Privacy design strategies. In *Proc. IFIP Int. Inf. Secur. Conf.*, pages 446–459.

Obaid, O. I. and Salman, S. A. (2022). Security and privacy in iot-based healthcare systems: A review. *Mesopotamian Journal of Computer Science*, 2022:29–39.

OWASP Foundation (2026). Threat modeling cheat sheet. https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html. Accessed: January 24, 2026.

Paim, J. et al. (2011). The brazilian health system: history, advances, and challenges. *The Lancet*, 377(9779):1778–1797.

Quincozes, V. E., Quincozes, S. E., Kreutz, D., Mansilha, R. B., and Kazienko, J. F. (2023). Information system for scheduling 4.0: Characterization, ux and lgpd. *iSys - Journal of Information Systems*, 16(1):5:1–5:31.

Sahi, M. et al. (2017). Privacy preservation in e-healthcare environments: A review. *IEEE Access*, 6:464–478.

Semantha, F. H., Azam, S., Yeo, K. C., and Shanmugam, B. (2020). A systematic literature review on privacy by design in the healthcare sector. *Electronics*, 9(3):452.

Severo, J. M., Herbert, J. S., and Franco, M. F. (2025). Threat modeling in healthcare: An analysis of trends, gaps, and emerging challenges. In *Anais da ERRC 2025: Artigos Completos do WRSeg*, pages 1–7.

Sion, L., Wuyts, K., Yskout, K., Scandariato, R., and Joosen, W. (2018). Interaction-based privacy threat elicitation. In *Proc. IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 79–86.

Wuyts, K., Sion, L., and Joosen, W. (2020). Linddun go: A lightweight approach to privacy threat modeling. In *Proc. IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*, pages 302–309.