Health Policy and Technology 10 (2021) 100576

Contents lists available at ScienceDirect

Health Policy and Technology

journal homepage: www.elsevier.com/locate/hlpt

# An analysis of the SICLOM information system employing misuse case diagrams

Bruno Marangoni dos Santos Leite [a,b,*], Marislei Nishijima [a,b], Flavia Mori Sarti [c], Marcos Lordello Chaim [d]

[a] Universidade de São Paulo, São Paulo, SP Brazil
[b] Institute of International Relations - University of Sao Paulo
[c] Universidade de São Paulo, São Paulo, SP Brazil
[d] Universidade de São Paulo, São Paulo, SP Brazil

ARTICLE INFO

*Keywords:*
Misuse case
ICT
HIV/AIDS
Information systems
Corruption

ABSTRACT

The World Health Organization (WHO) highlighted Information and Communication Technology (ICT) as a strategic tool to promote accessibility and guarantee efficiency to universal health systems. However, few studies evaluated the performance of information systems in developing countries. The paper aims to address the gap in the literature by assessing the SICLOM, a Brazilian information system used to manage the distribution of HIV/AIDS medication from the federal government to patients at the municipal level. Thus, we innovate by studying the potential flaws of SICLOM through the application of WHO's anti-corruption and transparency guidelines to the BPM Misuse Case diagrams. We documented several vulnerabilities that could be easily exploited to generate massive damage in the Brazilian HIV/AIDS program, patients, and government. Nevertheless, there is a trade-off between vulnerabilities and access to medication, in this case, facilitating access and creating opportunities for diversions in the system.

## Introduction

The advances of Information and Communication Technology (ICT) during the last decades fostered higher speed, traceability, and control of information flows in different areas. The health sector is a remarkable case in ICT applications from management of patients' medical records to decision support in complex diagnostic cases [1]. ICT is a strategic tool for promoting access and foster universal health systems, according to the World Health Organization (WHO) [2]. Its adoption is particularly important for health systems financed by the public sector, and ICT is supposed to promote efficiency and transparency in public governance.

ICT has been adopted to improve health systems both in developed countries, like the organisation for Economic Co-operation and Development (OECD) members [3], and developing countries, Brazil [4] and India [5]. However, there is lack of evidence evaluating the performance of ICT applied to health systems in developing countries. The studies previously published focused predominantly on the indirect performance of health systems ICT to foster development of health systems and improvement of patients' health outcomes [4,6].

Thus, the present study proposes to address the literature gap by investigating the performance of the Medicines Logistic Control System (SICLOM) in managing the processes for distribution of the antiretroviral drugs (ARV) - under the Brazilian Program for sexually transmitted diseases (STD), human immunodeficiency virus (HIV) and acquired immunodeficiency syndrome (AIDS) -, from the federal to the local governments, being delivered free of charge for patients.

The Brazilian Unified Health System (SUS) is publicly funded and offers universal health care for the population. The management and provision of health assistance through SUS was predominantly decentralized to the municipalities following the 1988 Brazilian Constitution. The federal government defines guidelines and funds health policies within the SUS, while states and municipalities provide health services and support part of the costs. Municipalities are responsible for providing primary care and financing payroll of health employees, states provide intensive care and fund additional health expenditures [7].

The Brazilian program for STD and HIV/AIDS was created in 1986 and merged to the SUS, operating in the decentralized primary care model after the 1988 Constitution. However, it remains an independent

* Corresponding author.
*E-mail addresses:* bruno-marangoni@alumni.usp.br (B.M.S. Leite), marislei@usp.br (M. Nishijima), flamori@usp.br (F.M. Sarti), chaim@usp.br (M.L. Chaim).

https://doi.org/10.1016/j.hlpt.2021.100576

Available online 8 November 2021

program regarding management [8]. The program's main costs refer to the ARV acquisition, due to the high prices of the medication, since major part of the program's activities involve providing HIV/AIDS treatment through distribution of medication for patients [8]. The program provided treatment for approximately 866,000 HIV-positive individuals in 2020 [9].

Under the decentralization logic, policies for HIV/AIDS program are defined by the central government, which also funds and purchases ARV to distribute to the municipalities. Municipalities, in turn, are in charge of providing health care services according to the local demand and the ARV are distributed for outpatient and inpatient treatments. Thus, SICLOM was developed to assist in medication logistic control, seeking to support the management of government funds, which represented the value of 1.58 billion of Brazilian Reais (approximately 395 million dollars) in 2019 [10].

The objective of the study was to identify potential system flaws in SICLOM, adopting an innovative strategy for analysis through combination of good practices in health care management guided by the WHO recommendations [2], applied to the Misuse Case tool of Business Process Modeling (BPM) [12], investigating whether its operation is efficient and secure.

## Context and literature review

Information is an input for planning, organization and management of services, monitoring, evaluation, and rearrangement of public health analysis at all government levels worldwide. The growing information for analysis in decision making processes requires its organization and systematization through information systems that improve its management [13].

National health systems rely on diverse coordinated activities, including delivery of medication. The pharmaceutical assistance cycle presents certain requirements to work properly, including appropriate management mechanisms that guarantee the necessary planning, resources, and infrastructure. These requirements must be based on an adequate and reliable information system [14].

The Brazilian Department for Surveillance, Prevention and Control of Sexually Transmitted Diseases, AIDS and Viral Hepatitis (STD-AIDS-VH) developed and implemented the SICLOM to meet these requirements, aiming at consistent and appropriate control of patients', health care facilities and medication data [15].

The SICLOM was created in 1997, based on a national registry of patients with HIV/AIDS under treatment within the public health system, which includes the history of the therapeutic schemes used and their effectiveness, as well as a set of statistics related to treatments and patients [15]. It also includes information of local ARV stocks to ensure prompt and adequate care in pharmacies located at the public health services, named Drugs Distribution Units (UDM).

Sahay and Puri [5] stress the need to obtain efficient technology of control to assist health systems. They conclude that even in the process of developing the computerized system used in the Indian healthcare system, acts of corruption were found given the government's political structure, creating opportunities for loss of efficiency in the whole system. Despite the concerns of the authors [5], there is absence of studies investigating vulnerabilities in the systems adopted within the Brazilian health system. Notwithstanding the literature gap, a huge scheme of corruption in the Brazilian government was recently disclosed in the country, named *Carwash Operation* [16].

Particularly referring to the Brazilian health system, the illustrative case of the *Fundacao para o Remedio Popular* (FURP) involved the public supply of medication. In 2019, FURP was investigated by a Parliamentary Investigation Commission due to irregularities in bidding processes with the government of the state of Sao Paulo [17]. The case illustrates potential deviations of medication using the health care budget within the Brazilian public sector. Regarding the ARV distribution, the incentives for similar deviations tend to be high since its prices are relatively higher than medication in other treatments supplied in a decentralized manner at primary health care units [8].

Several studies designed to detect vulnerabilities in ICT systems have demonstrated results through techniques focused on technical failures, while others focused on functional requirements [18,19]. The present study focused on the analysis of functional aspects of the SICLOM during the processes involved in distribution of medication.

Tools like Misuse Case diagrams showed substantial contributions in addressing security problems in process flows that are exclusively governmental in the Brazilian context, e.g., electronic voting [11]. This previous study demonstrated significant capacity of the Misuse Case tool to expose vulnerabilities of the system to stakeholders involved in the processes, using the brainstorm format. Thus, the lack of previous studies adopting the Misuse Case diagram to analyze information systems in any national health systems worldwide served as incentive for its adoption in the assessment of SICLOM.

## Methodological strategy and data

In 2018, the WHO started promoting anti-corruption, transparency and accountability in universal coverage health systems. To this end, a good practice guide was produced, named "Integrating a focus on anti-corruption, transparency and accountability in health systems assessments" [2]. The guidelines recommend good practices for improvement in health systems, proposing approaches for management and assistance in the diagnosis of areas under risk of corruption practices, and helping nations decide which anti-corruption, transparency and accountability methods should be used to improve efficiency.

The guidelines provide recommendations for several sub-areas of the health sector: service delivery; human resources for health; medical products, vaccines and technologies; health information systems; health financing; and governance. Although the guidelines address plans including the use of technology in a specific section referring to health information systems, we find that ICT may be also useful in other areas.

The WHO guidelines were adopted as indicative of situations and scenarios in which technology could help focusing on the medication distribution processes of the SICLOM. Therefore, we were able to have guidelines for good practices applied to ICT. The results allowed us to evaluate possible vulnerabilities of the system, considering its systemic flow, i.e., its functionally. The Misuse Case diagram was implemented to this end within the analysis.

According to Khan and Zulkernine [12], the Misuse Case is a special type of UML (Unified Modeling Language), a use-case diagram that describes the undesirable behavior of the software. It is a security requirement specification language describing a function that the system should not allow, e.g., a complete sequence of actions that might result in loss for the organization and its stakeholders. Alexander [20] defined it as an important tool for modeling and analyzing security scenarios, as it helps improve security and reduce threats.

Santos [21] observed that the Misuse Case diagram is composed of a mis-actor, an actor with malicious intent that initiates the flow. During modeling, use cases and actors must first be defined, followed by definition of misuse cases and mis-actors. The relationships between misuse cases and use cases may be identified in the diagram. Misuse cases and mis-actors are represented in solid black color to distinguish them from use cases and actors. Relationships with impediment and detection notation are used to associate use cases and misuse cases, indicating improper actions that must be prevented or detected. Then, new use cases must be specified to detect or prevent misuse case actions [21,8].

In addition to data from WHO guidelines, information from SICLOM was collected, corresponding to user guides made available by the government for system operators' orientation [10]. The user guides make it possible to understand the structure of system flows and thus apply the Misuse Case diagrams' elaboration.

## Results and discussion

The first step in analyzing the SICLOM was to provide a match for WHO guide (Table 1) to uncover potential opportunities for improvement in ICT. The results showed that the system has several vulnerabilities that may jeopardize the efficiency of the processes for ARV medication distribution in Brazil.

However, the proper description of the vulnerabilities and translation of its solutions in functional forms required the application of the Misuse Case tool for each case, as shown in Figs. 1–7.

Source: Elaborated by the authors from WHO guide.

Source: Elaborated by the authors from SICLOM.

Fig. 1 shows a case of vulnerability included in items 2, 5, and 6 of the WHO guidelines, originated by the lack of data consistency and mandatory consultation on the central government database to obtain patient information. This vulnerability occurs since the citizen's Identity Document is considered a weak identifier. Also, there are other competing individual identifiers er in the system. This vulnerability presents a risk of creating ghost users, purposely duplicated identifications or homonymous.

As a proposal to mitigate this point, we suggest making mandatory a consult of the patient in the SUS database (CadSUS), a national health system database that centralizes patients' information.

Source: Elaborated by the authors from SICLOM.

In the case B, Fig. 2, the vulnerability detected is framed at WHO guide in the items 3 and 6. It is originated by the absence of a blocking rule for the removal of medication for users without identification of SUS [10] in case of occupational exposure. This vulnerability is at risk of medication being withdrawn on behalf of users without their knowledge. As a proposal to mitigate this point, we suggest blocking the withdrawal function without identifying the SUS user.

Source: Elaborated by the authors from SICLOM.

Fig. 3 illustrates item C. In this case, the SICLOM vulnerability matches with items 3 and 4 of the guidelines. It is originated by the absence of a link between prescription and medication dispensing control. This vulnerability illustrates the risk of withdrawals in different amounts of drugs than the doctor's prescription. As a proposal to mitigate this point, we suggest creating a link or double-checking the revenue document by uploading the file on the SICLOM and subsequently be checked by a manager.

Source: Elaborated by the authors from SICLOM.

Regarding item D, Fig. 4, the vulnerability detected in the SICLOM matches items 1, 2, and 6 of the WHO guide, originated by the absence of a consultation portal for the patient to view their requests and history of medication withdrawals. This vulnerability is at risk of medication being withdrawn on behalf of users without their acknowledgement. As a proposal to mitigate this point, we suggest creating a portal to consult data on medication withdrawals using user SUS credentials and send an SMS alert to the patient.

Source: Elaborated by the authors from SICLOM.

With respect to item E, the vulnerability detected in the SICLOM matches items and 6 of the WHO guide, originated by the absence of systemic control for treatment abandonment in case of death. This vulnerability presents a risk of medicine deviation if the death is notified but not registered in the health system to remove the provision of medications. As a proposal to mitigate this point, we suggest creating integration with the Mortality Information System (SIM) to no longer require manual interaction.

Source: Elaborated by the authors from SICLOM.

Concerning item F, the vulnerability detected in the SICLOM matches item 5 of the WHO guide (Table 1), originated through the feature of medication possession control, called SUS user medicine possession", which allows partial medicine dispensation. This vulnerability presents the patient's risk declaring that he still has medication leftovers to obtain part of the prescription, and the health system agent purposely registering in the system as if the patient had withdrawn the whole

**Table 1**
SICLOM Vulnerabilities and the WHO good practices.

| Cause | Risk | Solution |
|---|---|---|
| 1. Long waiting and inefficient care scheduling, registration and patients' flow through the healthcare system. | It can create bribe opportunities even before a patient calls the clinical provider. | Mapping the scheduling processes, registration and patients' flow through the health system help to reveal bottlenecks that increase the risk of informal payments. |
| 2. Licensing and credentialing systems may be compromised by conflicts of interest or through bribery. | They can result in unqualified resources providing health services. | The evaluation team should ask key informants to share their perceptions. At the same time, however, it is important to be aware that weak systems may take time to be changed. |
| 3. Problems with fake prescriptions. | Medicines deviation (especially controlled substances and very expensive medication). | Evaluate systems to monitor stock or detect fake prescriptions or medication diversion schemes. Evaluation teams should consider whether the systems are ready to stop medication diversion (especially controlled substances or very expensive medication), and promptly identify diversion and intervene when this occurs. Health systems also need policies and procedures to investigate users' complaints and complaints about medication diversion, and manage actions if diversions are confirmed. Measuring stock shortages using samples is a way to detect possible diversion from medications. The inspection system must conduct random surveys. Health care workers should know that the unit can be inspected at any time, but not when. |
| 4. Prescribing clinicians having a financial conflict of interest regarding medication, or if there is evidence that prescribers may be receiving returns from laboratories or commercial representatives from the pharmaceutical industry. | Biased prescribing. | Ask whether prescribing clinicians are allowed to hold a financial interest in pharmacies or whether there is evidence that prescribers may be receiving kickbacks from pharmacies or industry sales representatives. If so, determine what controls are in place to prevent biased prescribing and ask about their functionality. Industry representatives may visit prescribers under the guise of education but really to try to generate business. Government policies to control industry influence on medical education should be considered. Finally, ask if the government requires |

(*continued on next page*)

**Table 1** (*continued*)

| Cause | Risk | Solution |
|---|---|---|
| | | industry to report gifts and other payments to doctors. |
| 5. Reports relying on fraudulent data or distorted by ghost facilities and ghost patients. Intentional fraud is a possible issue. Some contextual factors may lead to falsification of data, for example, an overdesigned and under-resourced information system staff who are asked to fill out too many forms. | Risk of fraudulent data. | Tools can help to triangulate data and shed light on risks of false data. For example, in Albania, the Government put in place a system whereby hospital patients receive a SMS after a facility visit, asking whether they received care and if they had to pay a bribe. Likewise, electronic procurement and open contracting systems may reduce opportunities to alter or suppress data. |
| 6. Stolen patient information. | Stolen patient information can be used for false billing by unscrupulous entities often posing as providers. | Explore and use electronic patient information protection to prevent theft. |

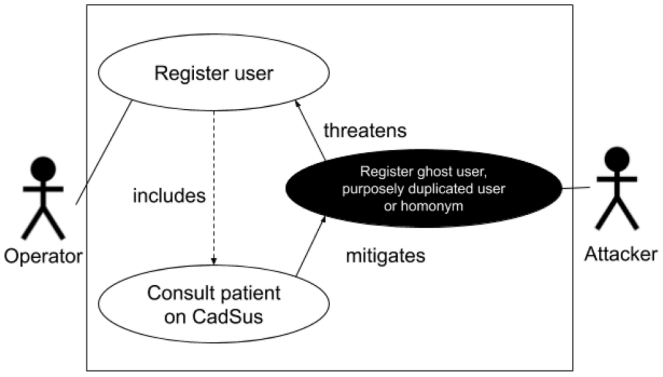


**Fig. 1.** SICLOM Misuse case diagram - Case A.

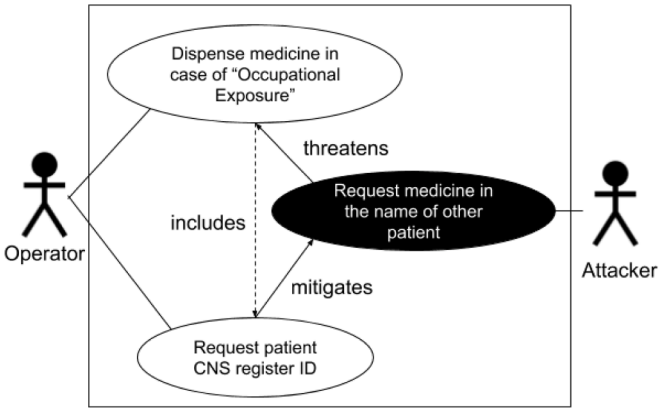


**Fig. 2.** SICLOM Misuse case diagram - Case B.

medication prescription. The correct thing to do in this scenario would be to launch as "SUS user medicine possession." As a proposal to mitigate this point, we suggest generating receipts signed by users with the actual amount of medication withdrawn and sending extract by SMS to users with the exact amount of medication withdrawn, as shown in the misuse case diagram in Fig. 6.

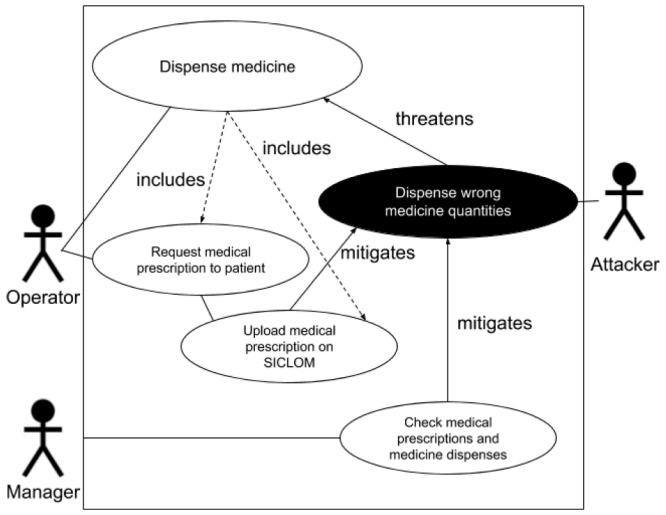


**Fig. 3.** SICLOM Misuse case diagram - Case C.

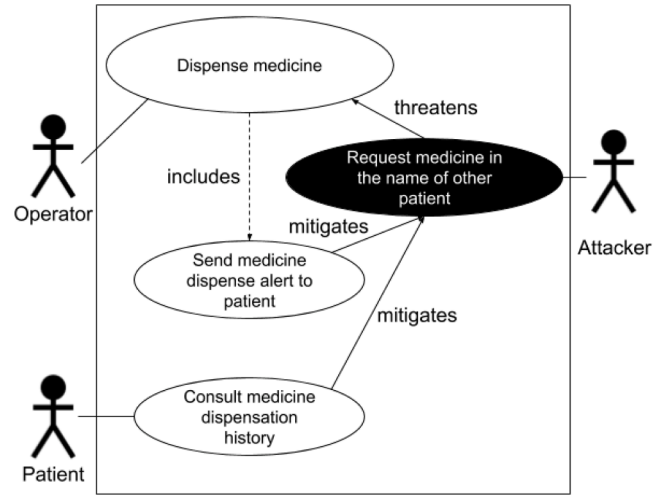


**Fig. 4.** SICLOM Misuse case diagram - Case D.

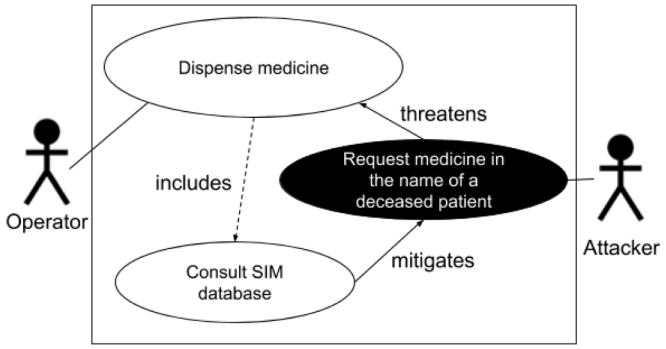


**Fig. 5.** SICLOM Misuse case diagram - Case E.

Source: Elaborated by the authors from SICLOM.

The vulnerability in the item G, Table 7, detected in the SICLOM matches items 3 and 6 of the WHO guidelines, originated by the lack of consistency of patient data when include in the category "hospitalized patient". This vulnerability poses a risk of medicine diversion through leakage of hospitalized patient data. As a proposal to mitigate this point, we suggest the creation of control with link between the SUS and the

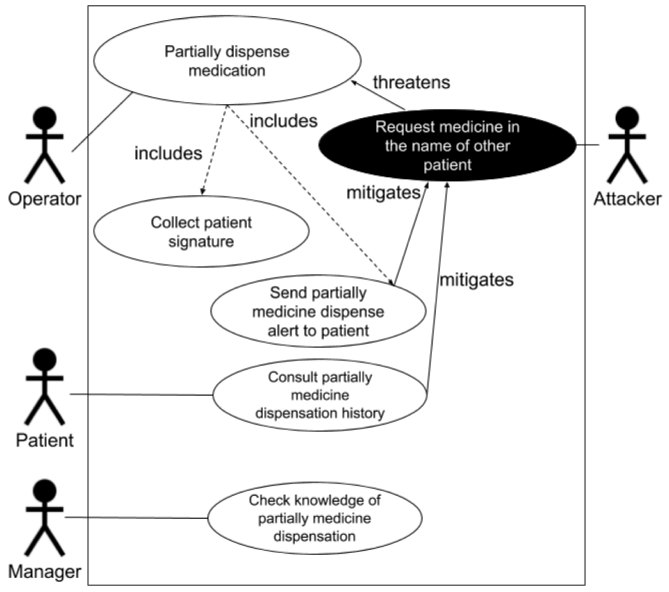


**Fig. 6.** SICLOM Misuse case diagram - Case F.

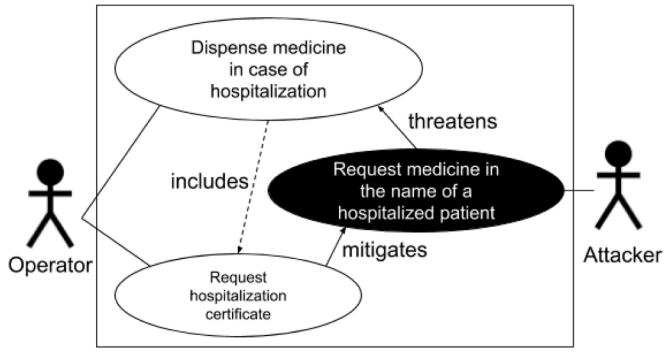


**Fig. 7.** SICLOM Misuse case diagram - Case G.

hospitals in order to validate and relate the data in case of hospitalization.

## Conclusion

SICLOM is an information system designed to manage the free distribution of ARV medication from the Brazilian central government to municipalities. The Misuse Case analysis on the SICLOM system identified several potential vulnerabilities that could risk the ARV medication distribution process. The vulnerabilities may compromise the Brazilian STD-HIV/AIDS program, its costs, and its efficiency due to the lack of accountability. Misuse Case diagrams also enabled the development of solutions that can mitigate threats represented by the vulnerable flows.

The analysis followed the WHO guide of good practices in health, which is intended to lead the countries to achieve efficient health systems, aiming to maximize capacity for assistance and promote universal health care coverage. Selecting six good practices in the WHO guidelines that were applicable to SICLOM allowed the assessment of SICLOM's adherence to good international practices.

The Misuse Case diagram proved to be a versatile tool for detecting vulnerabilities of SICLOM during the post-development process, allowing a precise diagnosis of the desired flow and potential malicious agents, and enabling to improve the SICLOM.

However, considering that the SICLOM was designed to assist patients simply and quickly, there is a trade-off in the system regarding security. While the Misuse Case points to several flaws in the system that could potentially comprise threats to the program, some flaws could allow the program to provide medicines for patients in situations that lack operationalization of full protocols, e.g., to distribute the ARV for the patient in the morning and register it in the afternoon due to the Internet connection problems.

Future studies should investigate whether malicious agents have exploited these vulnerabilities and, if they are occurring, how to bring evidence to the Brazilian government to allow further actions.

## Funding statement

We have no financial support to declare.

## Declaration of Competing Interests

We do not have competing interests to disclose.

## Ethical approval and consent

The study was based on secondary data obtained from the Department of Informatics of the Brazilian Unified Health System (DATASUS) and toolkit for assessment of health information systems of the World Health Organization (WHO), and there were no human subjects in the investigation, therefore, it is waived of the requirement of approval and sign of informed consent by the National Research Ethics Committee (CONEP).

## Acknowledgement

We thank Rosana T.V. Braga and the anonymous reviewers for the helpful comments. All errors are our own.

## References

[1] Kadiri SE, Grabot B, Thoben KD, Hribernik K, Emmanouilidis C, Cieminski GV, Kiritsis D. Current trends on ICT technologies for enterprise information systems. Comput Ind 2016;v79:14–33. https://doi.org/10.1016/j.compind.2015.06.008.
[2] World Health Organization. Global strategy on digital health 2020-2024. 2018. Available at, https://www.who.int/docs/default-source/documents/gs4dh0c510c483a9a42b1834a8f4d276c6352.pdf (accessed on February 14, 2021).
[3] Cette G, Lopez J, Presidente G, Spiezia V. Measuring 'indirect' investments in ICT in OECD countries. Econ Innov New Technol 2019;28(4):348–64. https://doi.org/10.1080/10438599.2018.1500105.
[4] Malaquias RF, Malaquias FFO, Hwang Y. The role of information and communication technology for development. Brazil, Inform Technol Develop 2017;23(1):179–93. https://doi.org/10.1080/02681102.2016.1233854.
[5] Sahay S, Puri S. The dynamics of corruption and ICT projects: case study from the public health system in India. In: ICIS 2008 Proceedings. 51; 2008. https://aisel.aisnet.org/icis2008/51 (accessed on September 15, 2017).
[6] Majeed MT, Khan FN. Do information and communication technologies (ICTs) contribute to health outcomes? An empirical analysis. Qual Quant 2019;53(1):183–206.
[7] Paim J, Travassos C, Almeida C, Bahia L, Macinko J. The Brazilian health system: history, advances, and challenges. Lancet North Am Ed 2011;377(9779):1778–97. https://doi.org/10.1016/S0140-6736(11)60054-8.
[8] Sarti F.M., Nishijima M., Campino A.C.C., Cyrillo D.C. A comparative analysis of outpatient costs in HIV treatment programs. Revista da Associação Médica Brasileira, 2012, 58(5):561–7. https://doi.org/10.1590/S0104-42302012000500013.
[9] Portela MC, Lotrowska M. Health care to HIV/AIDS patients in Brazil. Revista de Saúde Pública 2006;40:70–9. https://doi.org/10.1590/S0034-89102006000800010.
[10] SICLOM, Manuais. Available at http://azt.aids.gov.br. Accessed on Feruary 14, 2021.
[11] Whittle J, Wijesekera D, Hartong M. Executable misuse cases for modeling security concerns. In: ACM/IEEE 30th international conference on software engineering, Leipzig; 2008. p. 121–30.
[12] Khan M.U.A., Zulkernine M. A survey on requirements and design methods for secure software development. Queen's University School of Computing, Technical Report, 2009, no. 562.
[13] Pineo H, Zimmermann N, Davies M. Integrating health into the complex urban planning policy and decision-making context: a system thinking analysis. Palgrave Commun 2020;6:21. https://doi.org/10.1057/s41599-020-0398-3.
[14] Mabirizi D, Phulu B, Churfo W, Mwinga S, Mazibuko G, Sagwa E, Indongo L, Hafner T. Implementing an integrated pharmaceutical management information

system for antiretrovirals and other medicines: lessons from Namibia. Global Health 2018;6(4):723–35. https://doi.org/10.9745/GHSP-. -18-00157.
[15] Sakita KM. Avaliação da implantação do sistema de controle logístico de medicamentos/AIDS: o caso do distrito federal. Fundação Oswaldo Cruz, Escola Nacional de Saúde Pública Sergio Arouca; 2012. Master dissertation.
[16] Rotberg RI. (Org.), corruption in Latin America - how politicians and corporations steal from citizens. Springer Nature; 2019. https://doi.org/10.1007/978-3-319-94057-1.
[17] Agência Brasil, CPI apura irregularidades em fundação do remédio popular em São Paulo. Available at https://agenciabrasil.ebc.com.br/saude/noticia/2019-04/cpi-apura-irregularidades-em-fundacao-do-remedio-popular-em-sao-paulo (Accessed in February 14, 2021).
[18] Eusgeld I, Nan C, Dietz S. System-of-systems approach for interdependent critical infrastructures. Reliab Eng Syst Saf 2011;96(6):679–86. https://doi.org/10.1016/j.ress.2010.12.010.
[19] Hussain S, Honeth N, Gustavsson R, Sandels C, Saleem A. Trustworthy injection/curtailment of der in distribution network maintaining quality of service. In: 16th international conference on intelligent system applications to power systems, Hersonissos; 2011. p. 1–6. https://doi.org/10.1109/ISAP.2011.6082186.
[20] Alexander I. Misuse cases: use cases with hostile intent. IEEE Softw 2003;20:58–66.
[21] Santos LCMC. Uso de técnicas e ferramentas para detecção de vulnerabilidades: um survey com membros de equipes de desenvolvimento ágil de software. Universidade de São Paulo, Escola de Artes, Ciências e Humanidades da Universidade de São Paulo; 2018. Master dissertation.