





# Information security in healthcare supply chains: an analysis of critical information protection practices

## *Segurança da informação nas cadeias de suprimentos de saúde: uma análise das práticas críticas de proteção de informações*

Tiago Murer Furlanetto<sup>1</sup> , Edimara Mezzomo Luciano<sup>1</sup> , Odirlei Antonio Magnagnago<sup>1</sup> ,  
Rafael Mendes Lübeck<sup>1</sup> 

<sup>1</sup>Pontifícia Universidade Católica do Rio Grande do Sul – PUCRS, Programa de Pós-graduação em Administração, Porto Alegre, RS, Brasil. E-mail: tiagomf@gmail.com; eluciano@pucrs.br; odirlei@fag.edu.br; rafael.lubeck@pucrs.br

**How to cite:** Furlanetto, T. M., Luciano, E. M., Magnagnago, O. A., & Lübeck, R. M. (2020). Information security in healthcare supply chains: an analysis of critical information protection practices. *Gestão & Produção*, 27(4), e5376. <https://doi.org/10.1590/0104-530X5376-20>

**Abstract:** Because of their vital role and the need to protect the patient information, interest in information security in Healthcare Supply Chains (HSCs) is growing. This study analyzes how decisions related to information security practices in HSCs contribute to protecting patient information. Eleven semi-structured interviews were performed. The interviewees were managers from Brazilian HSC organizations. Four dimensions and 14 variables identified in a literature review were used to perform categorical content analysis. The findings suggest organizations, while aware of their critical information and internal processes, lack the necessary metrics to measure the impacts of possible failures. It seems organizations tend to invest in standard security measures, while apparently ignoring the specificity and complexity of information in HSCs.

**Keywords:** Supply chain management; Healthcare supply chain; Information security; Information security investments; Healthcare supply chain information.

**Resumo:** A cadeia de suprimentos de saúde da informação (HSC) está recebendo mais atenção por sua importância e também devido à crescente necessidade de proteger as informações dos pacientes. Esta pesquisa teve como objetivo analisar as práticas de segurança da informação que são predominantes no HSC para entender como as decisões nele contribuem para proteger as informações dos pacientes. Foram realizadas onze entrevistas semiestruturadas. Os entrevistados eram gerentes de organizações brasileiras de HSC. Quatro dimensões e 14 variáveis identificadas na revisão de literatura foram utilizadas para realizar a análise de conteúdo categórica. A principal descoberta foi que as organizações estão cientes de suas informações críticas e processos internos, mas não possuem as métricas necessárias para medir os impactos de possíveis falhas. As organizações investiram em medidas de segurança padrão, talvez, sem nenhuma preocupação particular com a especificidade e complexidade das informações no HSC.

**Palavras-chave:** Gestão da cadeia de suprimento; Cadeia de suprimentos de saúde; Segurança da informação; Investimentos em segurança da informação; Informações da cadeia de suprimento de saúde.

## 1 Introduction

Around the world, Information Technology (IT) is used in ever wider areas of life. Similarly, with business transactions, increasing numbers of individuals have access to information, without necessarily paying proper attention to its security. Such a lack of attention (Song et al., 2019) exposes organizations to information security breaches (Safa et al., 2016; Gordon et al., 2015). To defend themselves, organizations need to invest in information security, which is the protection of the organizational resources including information, hardware, or software (Chamikara et al., 2020; Guttman & Roback, 1995).

When organizations collaborate in supply chains, it is crucial to pay close attention to how their co-members deal with information security because if one fails, a breach can affect any and all the members of the chain (Gordon et al., 2015). Supply Chain Management (SCM) is considered vital for the success organizations pursuing profit and cost effectiveness while engaging with different suppliers (Ketchen & Hult, 2007).

There is an increased need to implement strong security measures to safeguard the information of organizations throughout the chain (Bojanc & Jerman-Blažič, 2008). However, the cost of the ideal information security protection system may impact their financial status. Thus, striking a balance between the costs of security measures and the value of information is a great challenge (Gordon & Loeb, 2002). Although it is far behind other industrial sectors in term of IT and SCM, this situation is no different in the healthcare sector (Chen et al., 2013; Hedström et al., 2011). IT has an increasingly important role in the field of healthcare assistance, due to the need to provide information in a timely manner for decision-making, as well as protect patient information. However, whatever of the cost of ensure information security, the cost of failing to protect patient information may be more expensive (Landolt et al., 2012; Samy et al., 2010). Healthcare professionals often require rapid access to patient information, and the delivery of that information may not always be in compliance with organizational and industry Information Security standards (Hedström et al., 2011; Huang et al., 2014).

Patient care and safety controls need to be established and abide by financial standards established by each organization (Huang et al., 2014). The challenge is to measure investments in Information Security against the impact of the failure of such systems (Huang et al., 2014).

Information Security is a technical discipline that aims to ensure maximum security levels (Bojanc et al., 2012). From among the various lines of research into Information Security, the present study adopts a behavioral approach to the issue (Zafar & Clark, 2009).

However, organizations need to consider the volume of security investments in order to assess whether the costs are feasible and whether they will provide the desired outcomes (Bojanc et al., 2012; Gordon et al., 2015). Furthermore, decision-makers must scrutinize how their supply chain members deal with Information Security (Huang et al., 2014).

A further challenge in Information Security lies in the growing number of daily transactions with different HSC members. Organizations are seeking faster and better healthcare information, nonetheless they must also consider the prospects for achieving better financial results (Huang et al., 2014; Hedström et al., 2011). In this context, this article seeks to answer: how decision-making in HSCs contributes towards protecting patients and if the actions taken are financially balanced?

## 2 Theoretical background

### 2.1 Information security

Organizations of all kinds are increasingly dependent on their IT resources for their business activities (Gordon & Loeb, 2002). IT systems have evolved from being operational to becoming strategic, including in supply chains (Gupta et al., 2006). The speed at which transactions take place today necessitates greater security measures for critical information (Gordon et al., 2015).

The primary goals of Information Security (IS) are the identification and the mitigation of possible security breaches in order to guarantee that, in the event of their occurrence, decision-makers will have enough information and knowledge to make the best decisions as fast as possible (Bojanc & Jerman-Blažič, 2008). While people are likely to fail in matters of security, it is the responsibility of IT to help users do the right thing, guiding them to make correct decisions from the security perspective (Kraemer & Carayon, 2007).

Due to the difficulty in determining the IT investment levels necessary to prevent failures, some managers have started to analyze the indirect results of security incidents in their organizations (Huang et al., 2014). This kind of investment analysis takes into account the value of the information, seeking to balance the cost of protecting the information against the costs involved in the case of information being leaked or unduly manipulated due to some breach (Bojanc & Jerman-Blažič, 2008). The analysis is sophisticated because there are many variables to be considered, such as the probability of a breach or failure (Patel et al., 2008; Huang et al., 2014).

By mapping all the critical business information for the organization, decision-makers can elaborate plans and analyze the relationships in order to optimize investments in information security (Gordon & Loeb, 2002; Gordon et al., 2015). When the cost of protection becomes too high, the organization may take out insurance to retrieve any possible losses in the case of information security breaches (Bojanc & Jerman-Blažič, 2008).

### 2.2 Supply chain management

A Supply Chain (SC) is a network of organizations that exchange information and products as a part of their business processes in order to deliver goods and services to their customers (Christopher, 2007). Since it is complicated for a single organization to perform all the production steps in a SC, SCM seeks to coordinate the relationships between organizations, splitting the processes and attributing each organization responsibility for specific steps that need to be taken to achieve the business goal (Ballou, 2006).

The primary objective of SCM is to ensure the efficiency of the SC to provide a competitive advantage to the member organizations (Christopher, 2007). To do so, the SCM has to plot strategies and processes that help the information and the products flow along the chain precisely in accordance with the needs of each organization (Ketchen & Hult, 2007).

For any organization, SCM is a critical factor in obtaining competitive advantage over others, whether to monitor the organization or to increase its efficiency (Gunasekaran et al., 2004). In this context, the financial aspect may be one of the key

indicators since it drives most of the decisions and is also used to measure chain performance (Gunasekaran et al., 2004; Christopher, 2007). However, the existence of vulnerabilities that might jeopardize information security along the SC cannot be ignored.

Research into HSCs has focused on improving their functioning and organizational results, preventing medical errors, ensuring better healthcare quality, and enhancing operational efficiency at hospitals (Lee et al., 2011; Kritchanchai et al., 2018).

Healthcare systems are constantly under pressure to reduce costs, while at the same ensuring better quality, and maintaining consistent levels of patient care (Kazemzadeh et al., 2012). Delivering healthcare assistance becomes difficult for hospitals if along with medical errors and patient information security, the costs of providing the service are high (Lee et al., 2011). SCM can help hospitals control these costs and so improve their financial performance (Lee et al., 2011; Wieser, 2011).

### **2.3 Information security on healthcare supply chains**

All the information that flows within an HSC is critical, for among other aspects, patient privacy. However, not all the employees affiliated with healthcare assistance organizations may fully understand that (Hedström et al., 2011; Magnagnagno, 2015). There is also a risk to organizational transactions, since details of agreements leaked on the market could damage the organizations involved, affecting their image or causing financial loss due to purchasing or delivery failures (Warren & Hutchinson, 2000; Gordon et al., 2015).

Healthcare assistance organizations have only recently started measuring the impacts of IS issues (Huang et al., 2014). However, when they need to choose between better financial results OR patient healthcare, they opt for the latter (Hedström et al., 2011). Investments in security entail increased organizational costs which need to be subjected to cost/benefit analysis (Chen et al., 2013). Moreover, such investments do not produce revenue, their value lies in their effectiveness in preventing information breaches, but this is not always identified or measured (Huang et al., 2014).

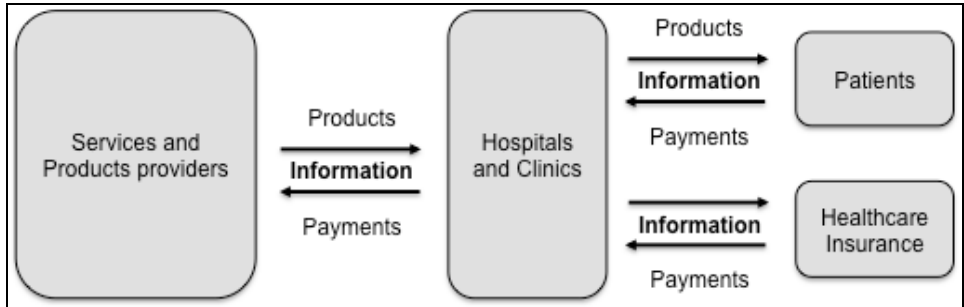
Typically, each organization seeks to apply its own information security method, which results in higher costs (Huang et al., 2014). However, given that the members of HSCs exchange information about patients, suppliers, materials, they should have better agreements regarding security since transferring such information poses greater risks than keeping it internally. Achieving a balance between ensuring sufficient security and the cost of providing that security is the crucial challenge (Warren & Hutchinson, 2000). Although there is considerable research into IS, vulnerabilities, and techniques, there is a lack of research into the financial aspects involved (Gordon & Loeb, 2002).

Information should not just be seen as an item that leads to increased costs, because its integrity is essential for all aspects of an organization's business processes (Bojanc et al., 2012). When the critical information is well identified, investment decisions regarding its security can be made (Gordon & Loeb, 2002; Gordon et al., 2015).

## **3 Conceptual model**

Organizations have focused on interorganizational processes (i.e., integrated with SC members) to achieve better organizational results and enhance efficiency in several

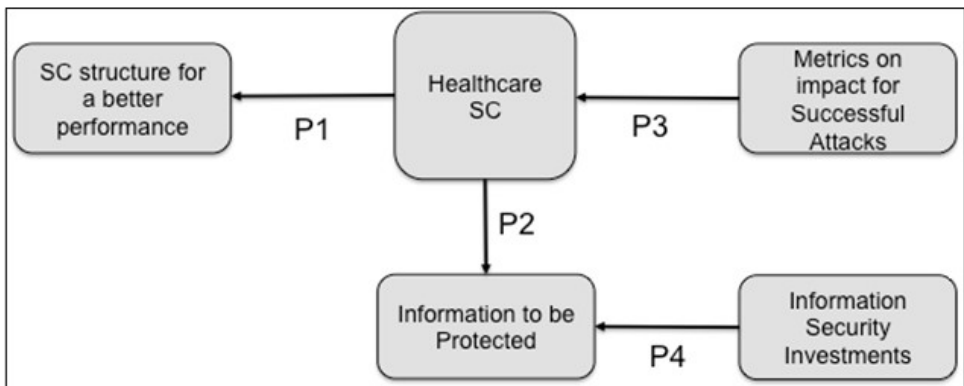
vital areas (Min & Zhou, 2002; Ballou, 2006). This kind of integration means critical information has to flow between the interconnected organizations, and that information needs to be secure, not only within a single company, but throughout the chain (Gomes & Ribeiro, 2004; Gordon et al., 2015). Figure 1 represents a model of a typical Brazilian HSC, which is also the theoretical model adopted in the present study:



**Figure 1.** Brazilian Healthcare Supply Chain. Source: Bhakoo & Chan (2011) and Kazemzadeh et al. (2012).

Patient healthcare product and service providers have direct access to hospitals and healthcare clinics (Kazemzadeh et al., 2012). They provide all the products and medicines necessary for healthcare organizations to provide assistance to patients (Bhakoo & Chan, 2011). In Brazil, numerous organizations offer health insurance to cover their customers’ healthcare costs. (Magnagnagno, 2015).

Given the HSC structure presented in Figure 1, it is important to understand the Information Security initiatives applied both within the member organizations and throughout the HSC. Based on that, the conceptual model presented in Figure 2 was created.



**Figure 2.** Conceptual Model. Source: The authors.

Assuming HSC are behind SCs in other industrial sectors (Chen et al., 2013; Hedström et al., 2011), this article uses the conceptual model to explore the Information-Security-related activities of SC organizations using HSC to validate propositions. SCs seek to manage processes among their member organizations in an integrated fashion order to yield better results in terms of their operations, products, services, and information (Ballou, 2006; Gunasekaran & Ngai, 2004).

In turn, Ayers (2006) addresses the sharing of information, with the function of generating a flow of knowledge to satisfy the requirements of the end user. For this, it is necessary to take into account the possibility and the great need for a relationship between all companies from different sectors that will participate in the process (Cooper et al., 1997).

On the other hand, organizations face a very big challenge to promote security standards, policies and procedures effectively (Boss et al., 2009). Due to the great complexity of security, to stay safe, it is necessary to pay attention to the configuration of all levels of users and also to the systems (Marciano, 2006).

Given that, the first proposition is: **(P1) Information Security among organizations in HSCs is integrated and collaborative.**

Effective decision-making is based on information, and systems are necessary to handle all the information needed. Therefore, it is crucial the information is accurate and secure (Bragança, 2010; Bojanc & Jerman-Blažič, 2008; Warren & Hutchinson 2000; Gordon et al., 2015). In HSCs, huge volumes of patient, treatment and supplier information flows along the chain (Ballou, 2006). Hence, the second proposition is: **(P2) Organizations are aware of the need to protect their critical information and, that the HSC is a vital part of that.**

Organizations use performance metrics to help them achieve better organizational results, while, at the same time, they also have to protect their information (Gunasekaran & Ngai, 2004). Organizations need to consider the possibility of IS breaches and their impact on financial results (Bojanc & Jerman-Blažič, 2008; Gordon & Loeb, 2002). Hence, the third proposition is: **(P3) Organizations have metrics to assess the impact of information security breaches.**

Besides strategic and financial information, HSCs deal with sensitive patient data that has to be both secure and constantly available to the professionals directly delivering medical assistance (Ballou, 2006; Bragança, 2010). Each organization's critical information needs to be identified to ensure suitable protective measures can be taken (Bojanc & Jerman-Blažič 2008; Huang et al., 2014). Therefore, the fourth proposition is: **(P4) Specific investments are made to properly protect both the organization's and HSC's critical information.**

## 4 Methodology

This qualitative study is intended to reveal the interviewees' views regarding IS-related SCM initiatives. It does not offer well-defined pre-concepts, but rather makes four non-precise propositions (Gibbs, 2009; Sampieri et al., 2013) that hopefully will be answered in the course of the interviews and the subsequent interpretation by the researcher (Gibbs, 2009; Sampieri et al., 2013).

The units of analysis are the professionals themselves and their particular view of the organization, considering the environment in which they work and the external relations with other organizations.

### 4.1 Research instrument

At the core of the research instrument are four dimensions and a set of variables that were created based on the conceptual model and the theoretical background.

Table 1, below shows the dimensions and their related goals, the variables, and the pertinent literature.

**Table 1.** Dimension Matrix.

<b>Dimensions and goals</b>	<b>Variables</b>	<b>Sources</b>
<b>SC processes for better information flow</b>	a) Internal information flow;	SCC (2010), Min & Zhou (2002), Gunasekaran et al. (2001), Croom et al. (2000), Christopher (2007), Chen et al. (2013), Ballou (2006)
Identification of the organization's role and the information that flows within the chain	b) Information flow among members;	
	c) Role of the organization within the SC;	
	d) Definition of members and relations.	
<b>Information to be secured</b>	a) What is the critical information that needs to be secured;	Warren & Hutchinson (2000), Guttman & Roback (1995), Gunasekaran et al. (2004), Gordon et al. (2010), Gomes & Ribeiro (2004), Gaunt (2000), Chen et al. (2013), Bojanc & Jerman-Blažič (2008)
Analysis of how the organizations in the SC transition critical information	b) How information is accessed;	
	c) How information is exchanged among members.	
<b>Threats and mitigating actions</b>	a) Recognition of threats and their impacts	Warren & Hutchinson (2000), Ten et al. (2008), Patel et al. (2008), Gordon et al. (2015), Gaunt (2000), CERT (2015), Bojanc & Jerman-Blažič (2008), Bojanc et al. (2012), Safa et al. (2016), Huang et al. (2014)
Identification of how organizations understand the threats, and their actions to mitigate them	b) Mitigation actions on Information Systems;	
	c) Mitigation actions on employees;	
	d) Information monitoring.	
<b>Information Security investments</b>	a) To evaluate the impact of threats;	Warren & Hutchinson (2000), Ten et al. (2008), Huang et al. (2014), Gupta et al. (2006), Gordon & Loeb (2002), Bojanc et al. (2012)
Analysis of how organizations define their Information Security budget.	b) Specific Information Security budget;	
	c) Investment impact on the organization and SC financial performance.	

Source: The authors.

The instrument was validated in a process involving two respondents, one from the academic field, with a background both in Information Systems and healthcare, and the other was an IT manager from a hospital.

## 4.2 Data collection

This study sought to analyze the answers provided by professionals from the organizations in HSCs. The selected interviewees were from general management areas in their respective organizations, namely laboratories, hospitals, clinics, and healthcare insurance providers, operating within HSCs.

The study focuses on the interviewees and their knowledge about Information Security and the HSCs to which their organizations belong with the aim of identifying the relevant IS practices and SC processes (Flick & Netz, 2004).

All the included organizations were members of HSCs operating in two different cities in the Southern States of Brazil. Among the 11 specialists from 10 different organizations that agreed to be interviewed, 3 were from IT departments, and 8 from management. All the interviews were held and recorded between October and November 2015, and later transcribed and analyzed.

### 4.3 Data analysis

The content analysis was conducted according to Bardin, Bardin et al. (1979), using the following three steps: (i) pre-analysis; (ii) exploration of material; (iii) result processing, inference, and interpretation.

The first step, (i), involved transcribing the interviews. The second step, (ii), involved the use of NVivo software to obtain a better view of the data and to group answers. The third step, (iii), required the researcher to interpret the data. This last stage consisted of categorical analysis, initially openly coding the data to identify prior categories based on the transcripts. After which, axial analysis was performed to group the comments according to similarity. Finally, careful analysis was carried out to identify the final categories, which also made it possible to establish their frequencies (Sampieri et al., 2013). The data from each interviewee were then compared with that obtained from the other interviewees as well as with the literature in order to validate the answers (Flick & Netz, 2004).

## 5 Results

### 5.1 Characterization of the respondents

A total of 11 professionals from the HSCs were interviewed. Their characterizations presented in Table 2.

**Table 2.** Characterization of respondents.

Code	Organization	Age	Formation	Role	No. of Employees
I1	Laboratory A	62	Medicine	CEO – Owner	Up to 100
I2	Laboratory B	45	Pharmacy	CEO	101 to 500
I3	Clinic	30	IT	IT Manager	Up to 100
I4	Hospital A	37	Hospital Administration	Administrative Manager	Up to 100
I5	Hospital A	39	IT	IT Manager	Up to 100
I6	Hospital B	50	Hospital Administration	Manager - Owner	101 to 500
I7	Hospital C	37	Administration	Manager	501 to 1000
I8	Hospital D	43	Administration	Executive Director	501 to 1000
I9	Hospital E	22	IT	System Administrator	101 to 500
I10	Hospital F	40	Hospital Administration	Board Technical Consultant	More than 2000
I11	Healthcare Insurance	47	Hospital Administration	Operations Manager	101 to 500

Source: Collected Data (2016).



## 5.2 Proposition analysis

### 5.2.1 Proposition 1 – Information security among organizations in HSCs is integrated and collaborative

This proposition suggests that the organizations act in an integrated manner in seeking to achieve better organizational results. Nevertheless, the interviewees suggested this was not the usually case, for example I2 said: *“We have many opportunities, but we live on different islands. We should be on the same land...that is what I stand for. The closer we get, the better the SC performance will be...”*

On the same subject, I11 suggested SC members cheat on each other, and on hospitals, and laboratories, performing more exams than necessary. So, he pays less for each service to compensate. He said, *“I cannot pay more for their services, because they do more than necessary, and they do more because they think I am not paying enough. So, everyone loses”*.

The proposition that all the organizations seek better organizational results is confirmed. However, they do it individually, with low levels of integration and collaboration, even among organizations in the same HSC. They maintain a relationship focusing exclusively on the supply of services and the materials they need to perform their activities.

### 5.2.2 Proposition 2 – Organizations are aware of the need to protect their critical information and, that the HSC is a vital part of that

The interviewees agreed that the security of patient information was critical throughout the HSC. The importance of the commercial contracts between the members was also noted.

Interviewee I8 referred to the critical nature of patient information: *“...Medical records, for sure, are the critical, and are even protected by law...”* However, he also mentioned the commercial information in the following statement: *“...Price is critical; if my competitors discover the amounts I pay, they can force my supplier to accept the same or change mine...”* Interviewee I7 agreed upon this opinion, but not with I10, who claimed there is no confidentiality request between his hospital and its suppliers.

Organizations need to be aware of their critical information for them to work effectively and to achieve any competitive advantage in the market (Bojanc & Jerman-Blažič, 2008). Once the critical information is identified, they can focus their efforts to protect it (Bojanc et al., 2012). Patient information is the most critical, not only because of the legal implications involved but also due to the possible indirect negative impact on the organization (Hedström et al., 2011; Huang et al., 2014). Proposition 2 was confirmed. The organizations indeed know which information is critical for them and for the HSC to which they belong.

### 5.2.3 Proposition 3 – Organizations have metrics to assess the impact of information security breaches

This proposition suggests the organizations always have metrics to measure the impacts they, as well as the HSC they belong to, would face when confronted by information security breaches.

Interviewee I3 said that the whole chain faces many security issues. *“...Today, banks have advanced security systems and even so, they suffer attacks...the healthcare area does not invest as much as them...”* When asked why that is the case, he suggested, *“...Maybe due to misinformation about what could happen. Maybe studies could show them how vital this information is.”*

I3 elaborated on the answers found in most of the interviews, which showed they were aware of the possible impacts of an information breach. Nevertheless, neither I3 nor the other interviewees had any real data to support their assumptions and had little idea of the damage that would be caused to the organization or the HSC. That was the main reason most of them felt the most significant impact would be on the organizational image, but they were unable to translate that feeling into real numbers. However, the categorical analysis shows that “immeasurable damage” was the most frequent term used.

The interviewees are aware of the impacts an information security breach would have on their organizations. However, they have no idea of the possible magnitude, thus, they cannot make suitable plans to mitigate such an event. The third proposition was not confirmed.

#### **5.2.4 Proposition 4 – Specific investments are made to properly protect both the organization’s and HSC’s critical information**

The last proposition was intended to cross-check the previous ones in terms of Information Security investments. It suggests the organizations invest in security actions according to the information they need to protect.

Proposition 1 was partially confirmed due to the low level of integration between the organizations. Proposition 2 was confirmed; the organizations know what information is critical for them and for the HSC. Proposition 3 was not confirmed since the organizations had no metrics to measure the impact of any information security breach. Consequently, proposition 4 shows the organizations invest in information security, but they do so on an individual basis rather than in a coordinated manner with the whole HSC, nor do they consider the criticality of the information itself.

Every organization should invest in IS according to the value of the information that they want to protect (Bojanc & Jerman-Blažič, 2008). In HSCs, there is critical information that is protected by law (according to I8). Nevertheless, there is no assessment of the costs that would be incurred in the case such information is compromised. Hospital managers need to be aware of the kind of information they are dealing with in order to make plans to prevent breaches of IS and mitigate their impacts in the case they occur, while ensuring the costs of any IS system designed to do so does not exceed the value of the information it is intended to protect (Huang et al., 2014).

Interviewee I10 commented that the hospital always takes action reactively. After a breach occurs, they attempt to identify the best means of preventing it from reoccurring and mitigating its impact. Interviewee I9 says they do the same, but he adds that if they conducted prior risk analysis they might be able to prevent breaches and, thereby, avoid financial losses.

Compared to SCs in other sectors, such as manufacturing, there is much to be studied regarding HSCs (Chen et al., 2013). However, that does not mean IS in HSCs also has to lag behind, because healthcare involves highly personal information. Depending on

the seriousness of the breach, it could mean the end of a healthcare assistance organization (Hedström et al., 2011; Landolt et al., 2012; Huang et al., 2014).

### 5.3 Analysis of the dimensions and variables

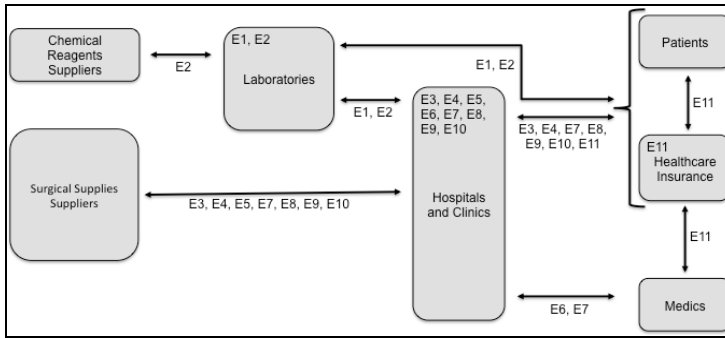
All the variables identified in the literature review are analyzed in the transcript data. Below, Table 3 shows the results of the analysis of the dimensions and variables.

**Table 3.** Variables Analysis.

Dimension	Variable	Results
SC processes for better information flow	Internal information flow	Main categories identified refer purchasing and product tracking
	Information flow between members	The results point to a low level of integration between members
	Role of the organization within the SC	With a low level of integration, the organization focuses on internal processes
	Member's definition	They know their co-members. The diagram can be seen in Figure 2
Information to be protected	Critical information to be secured	Medical records and patient data are the most critical information in the HSC
	Information access	Individual access is limited accordingly to the user's role
	How information is exchanged among members	The main category was E-mail/Website, but the clinic and the hospital also had identified systems
Threats and mitigation actions	Recognizing the threats and their impacts	The main threats include information leak, information unavailability, and internal threats. However, there is no analysis of the impacts
	Mitigation actions in information systems	The main categories identified concern the use of purchased systems, which are considered safer than the in-house systems, and the use of backups
	Mitigation actions on employees	Organizations have codes of conduct and contractual obligations, but they are not periodically reviewed
	Information monitoring	The interviewees said that they know it exists, but only a few were able to specify
Information Security investments	To assess the impact of threats	Organizations have no formal IS breach impact analysis procedures.
	Specific Information Security budget	There is no specific IS investment, only those recommended by IT
	Impact of investment on the organization, and the financial performance of the SC	There is no analysis to validate the amount spent on Information Security and its impact on the organizational performance

Source: The authors.

The variable 'member's definition' considers the organization's suppliers and clients within the HSC. Figure 3 presents the SC diagram according to the responses of the interviewees. Each arrow shows interviewee (e.g. E2/I2) whose comments support the connection.



**Figure 3.** Healthcare Supply Chain Identified in the Study. Source: Research Data (2016).

With one exception, all the interviewees agree and have similar views regarding the HSCs. They understand their own and their co-members’ roles. The only disagreement was with respect to the physicians. Some interviewees consider themselves as clients, others as service providers. According to I8, this may occur because they work inside organizations, which camouflages their real role within the HSC. So, the question arises: Are they employees, service providers, or clients?

### 5.4 Discussion

The main research question asked whether the organizations within HSCs identified their critical information and whether they had the necessary processes in place to adequately protect that information, while considering the value of the information and the cost of protecting it. Based on the interviews, it can be concluded the healthcare organizations are aware of their critical information, but there is neither any standard process in place nor any analysis being done in order to properly protect the information. Table 4 provides a summary of the results for each dimension as previously defined.

**Table 4.** Summary per Dimension.

Dimension	Results
SC processes for better information flow	The individual organizations have defined internal processes, but not for the whole HSC. The level of the relations and level of integration and shared activities are even lower.
Information to be protected	The information related to patients is the most critical in the HSC, and the organization performs mitigation actions to protect it.
Threats and mitigation actions	The main threats identified include information leaks, information unavailability, and internal breaches. However, organizations keep their systems up to date; they have codes of conduct, but these are not regularly reviewed and emphasized to the employees.
Information Security investments	There is no analysis regarding the impact of possible information breaches and no specific investment to safeguard against them. They only carry out the standard processes suggested by IT their departments without conducting risk or cost/benefit assessments considering the losses that would be incurred in the case of information security breaches.

Source: The authors.

Overall, the primary information in HSCs is patient-related. All the interviewees imagined the impact on their respective organizations in the case of a security breach

would be significant. Nevertheless, no risk analysis had been conducted in terms of the organizations or the HSCs. Although at a low level of integration, some information is shared among member organizations, nevertheless there is no analysis is made to measure it. Figure 4 presents the author's perspective on the levels of IS between the connections in the HSC.

- High Level in terms of Information Security Practices (HL ISP): There are some security protocols, integration systems, and low levels of information shared by unsecured channels;
- Medium Level in terms of Information Security Practices (ML ISP): There is some integration through systems, but high information is shared by insecure channels, such as emails and printed documents;
- Low Level in terms of Information Security Practices (LL ISP): Information is shared mainly through unsecured channels.



**Figure 4.** Identified Levels on SI Practices in Healthcare SCs. Source: The authors.

According to the data collected, HSCs do not seem relevant to the results pursued by the organizations. They recognize the need for members, but they do not have close relationships and do not help each other achieve better performance for all the co-members. They have weak ties and little trust in each other, sometimes even hiding information, being afraid their co-members might take advantage of them rather than work together to achieve better results.

The study revealed the interviewees' concerns about information privacy, mainly regarding the medical teams that needs to access the patient information. Reports of the low level of concern for patient privacy by medical teams are not new. Related to information privacy, Luciano et al. (2011) suggest the most worrying aspects involve the wide range of the professionals/people that have access to patient information and what they are can and cannot do with it. This concern is expressed by I9 who says the doctors are resistant to having exclusive access to patient data. They want the medical team members to have access to patient information, but not all such members need to have access to all the information.

Regarding investments in information security, it was found the organizations do not consider the value of the information when deciding how much they will spend on protecting it, nor do they consider the impact on the/organization in the case of information security breaches. The organizations purchase information security products available on the market, without focusing on the nature of their critical information, despite the possible consequences they would face in case of information security breaches.

## 6 Final remarks

Healthcare managers are increasingly concerned with the financial health of the medical institution to maintain their level of assistance and increase their capacity to attend patients (Lee et al., 2011). This study has analyzed the critical information in HSCs together with the practices related to IS investments made to protect that information in the HSC and the perception of the impact of those investments on the organizational performance of the organizations and the HSCs.

The findings help explain the four research propositions, and, to some extent, are in line with those reported in previous studies. Among the findings, is that the internal hospital supply chains are defined and coordinated than the external supply chains. The hospitals have several security practices in place, such as individual access to systems, access profile levels, as well as contractual obligations and employee conduct guidelines. They also have backup procedures in place, and some even have redundancy systems. In addition, hospitals have transparent procurement processes for their materials and medicines. Rigorous tracking systems for all the products are necessary to increase the quality and the security of their use.

This study's primary objective was to analyze IS practices in relation to protecting critical information within HSCs. The findings suggest the adopted information security practices are not based on the critical information in each organization and much less so on the relations with other organizations in the HSC. The organizations tend to make global IT investments that can, consequently, impact information security. Despite their importance, they are not based on risk and cost/benefit assessments regarding the value of the information or the impact in the case of information security breaches. That also implies unknown factors related to the impact of the investments on the organizational financial performance and, consequently, on the financial performance of the HSCs.

Despite which, the levels of integration and collaboration among the members are very low, thus limiting their capacity to achieve the kind of efficiency levels and results expected of a successful SC. They are concerned about information security but do not analyze the issues that may arise in the case of breaches. Consequently, they do not have the correct information to make better decisions to safeguard their information.

How the members of HSCs and their co-members deal with information is mapped in Table 3 and summarized in Table 4. This includes the SC processes and critical information mapping, which is consistent regarding patient data, threats and mitigation mapping and their strategies for IS investments.

This study also contributes by examining how investments in Information Security impact the organizational performance of the organizations and the HSCs. While some studies in this area have looked at healthcare organization security, their focus is on patient privacy, as in Bragança (2010) and Magnagnagno et al. (2015). They analyze the organization alone and do not consider the financial aspects of security investments.

In Brazil, there is a considerable amount of research into the healthcare area. The findings of present study suggest insufficient attention has been given to SCM, particularly in terms of risk and cost/benefit assessments regarding investments in information security and the impacts of information security breaches. Consequently, there is no security investment analysis regarding the critical information they handle every day. These findings should be taken into account by HSC and/or SC Information Security managers when analyzing the possible impacts related to information breaches and planning future investments designed to protect the organization and the

HSC of which they are a part. This study has two main limitations, namely the number of interviewees and the low level of integration among the organizations in the HSCs. Some suggestions for future research based on the results are:

- Applying the research instrument in other regions;
- Conducting quantitative research in order to get a higher number of responses. So, the data can be analyzed statically in order to be able to generalize the results;
- Creating a governance-integrated model for Information Security in HSCs;
- Developing a base model for Information Security for organizations within HSCs, with possible impacts and losses, so organizations could prioritize their investments.

This study has analyzed the prevalent practices intended to protect critical information in HSCs. The lack of coordination of information security practices among the organizations in the HSCs is something that should be revised.

## References

- Ayers, J. B. (2006). *Handbook of supply chain management*. Boca Raton: Auerbach.
- Ballou, R. H. (2006). *Gerenciamento da cadeia de suprimentos/logística empresarial* (5. ed.). Porto Alegre: Bookman.
- Bardin, L., Reto, L. A., & Pinheiro, A. (1979). *Análise de conteúdo*. Lisboa: Edições 70.
- Bhakoo, V., & Chan, C. (2011). Collaborative implementation of e-business processes within the health-care supply chain: the Monash Pharmacy Project. *Supply Chain Management*, 16(3), 184-193. <http://dx.doi.org/10.1108/13598541111127173>.
- Bojanc, R., & Jerman-Blažič, B. (2008). An economic modeling approach to information security risk management. *International Journal of Information Management*, 28(5), 413-422. <http://dx.doi.org/10.1016/j.ijinfomgt.2008.02.002>.
- Bojanc, R., Jerman-Blažič, B., & Tekavčič, M. (2012). Managing the investment in information security technology by use of a quantitative modeling. *Information Processing & Management*, 48(6), 1031-1052. <http://dx.doi.org/10.1016/j.ipm.2012.01.001>.
- Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, 18(2), 151-164. <http://dx.doi.org/10.1057/ejis.2009.8>.
- Bragança, C. E. B. A. (2010). *Privacidade em informações de saúde: uma análise do comportamento percebido por profissionais de saúde de instituições hospitalares do Rio Grande do Sul* (Dissertação de mestrado). Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre.
- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT. (2015). Retrieved in 2015, April 1, from <http://www.cert.br/>
- Chamikara, M. A. P., Bertok, P., Liu, D., Camtepe, S., & Khalil, I. (2020). Efficient privacy preservation of big data for accurate data mining. *Information Sciences*, 527, 420-443. <http://dx.doi.org/10.1016/j.ins.2019.05.053>.
- Chen, D. Q., Preston, D. S., & Xia, W. (2013). Enhancing hospital supply chain performance: a relational view and empirical test. *Journal of Operations Management*, 31(6), 391-408. <http://dx.doi.org/10.1016/j.jom.2013.07.012>.
- Christopher, M. 2007. *Logística e gerenciamento da cadeia de suprimentos: criando redes que agregam valor* (2. ed.). São Paulo: Thomson Learning.

- Cooper, M. C., Lambert, D. M., & Pagh, J. D. (1997). Supply chain management: more than a new name for logistics. *International Journal of Logistics Management*, 8(1), 1-14. <http://dx.doi.org/10.1108/09574099710805556>.
- Croom, S., Romano, P., & Giannakis, M. (2000). Supply chain management: an analytical framework for critical literature review. *Journal of Purchasing and Supply Management*, 6(1), 67-83. [http://dx.doi.org/10.1016/S0969-7012\(99\)00030-1](http://dx.doi.org/10.1016/S0969-7012(99)00030-1).
- Flick, U., & Netz, S. (2004). *Uma introdução à pesquisa qualitativa*. Porto Alegre: Bookman.
- Gaunt, N. (2000). Practical approaches to creating a security culture. *International Journal of Medical Informatics*, 60(2), 151-157. [http://dx.doi.org/10.1016/S1386-5056\(00\)00115-5](http://dx.doi.org/10.1016/S1386-5056(00)00115-5). PMID:11154966.
- Gibbs, G. (2009). *Análise de dados qualitativos: coleção pesquisa qualitativa*. Porto Alegre: Bookman.
- Gomes, C. F. S., & Ribeiro, P. C. C. (2004). *Gestão de cadeia de suprimentos integrada à tecnologia da informação*. São Paulo: Pioneira Thomson Learning.
- Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4), 438-457. <http://dx.doi.org/10.1145/581271.581274>.
- Gordon, L. A., Loeb, & Sohail, (2010). Market value of voluntary disclosures concerning information security. *Management Information Systems Quarterly*, 34(3), 567-594. <http://dx.doi.org/10.2307/25750692>.
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model. *Journal of Information Security*, 6(1), 24-30. <http://dx.doi.org/10.4236/jis.2015.61003>.
- Gunasekaran, A., & Ngai, E. W. T. (2004). Information systems in supply chain integration and management. *European Journal of Operational Research*, 159(2), 269-295. <http://dx.doi.org/10.1016/j.ejor.2003.08.016>.
- Gunasekaran, A., Patel, C., & McGaughey, R. E. (2004). A framework for supply chain performance measurement. *International Journal of Production Economics*, 87(3), 333-347. <http://dx.doi.org/10.1016/j.ijpe.2003.08.003>.
- Gunasekaran, A., Patel, C., & Tirtiroglu, E. (2001). Performance measures and metrics in a supply chain environment. *International Journal of Operations & Production Management*, 21(1-2), 71-87. <http://dx.doi.org/10.1108/01443570110358468>.
- Gupta, M., Rees, J., Chaturvedi, A., & Chi, J. (2006). Matching information security vulnerabilities to organizational security profiles: a genetic algorithm approach. *Decision Support Systems*, 41(3), 592-603. <http://dx.doi.org/10.1016/j.dss.2004.06.004>.
- Guttman, B., & Roback, E. A. (1995). *An introduction to computer security: the NIST handbook*. Gaithersburg: National Institute of Standards and Technology.
- Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, 20(4), 373-384. <http://dx.doi.org/10.1016/j.jsis.2011.06.001>.
- Huang, C., Behara, R. S., & Goo, J. (2014). Optimal information security investment in a Healthcare Information Exchange: an economic analysis. *Decision Support Systems*, 61, 1-11. <http://dx.doi.org/10.1016/j.dss.2013.10.011>.
- Kazemzadeh, R. B., Sepehri, M. M., & Jahantigh, F. F. (2012). Design and analysis of a health care supply chain management. *Advanced Materials Research*, 433-440, 2128-2134. <http://dx.doi.org/10.4028/www.scientific.net/AMR.433-440.2128>.
- Ketchen, D. J., Jr., & Hult, G. T. M. (2007). Bridging organization theory and supply chain management: the case of best value supply chains. *Journal of Operations Management*, 25(2), 573-580. <http://dx.doi.org/10.1016/j.jom.2006.05.010>.



- Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics*, 38(2), 143-154.
- Kritchanchai, D., Hoes, S., & Engelseth, P. (2018). Develop a strategy for improving healthcare logistics performance. *Supply Chain Forum: An International Journal*, 19(1), 55-69. <http://dx.doi.org/10.1080/16258312.2017.1416876>.
- Landolt, S., Hirschel, J., Schlienger, T., Businger, W., & Zbinden, A. M. (2012). Assessing and comparing information security in Swiss hospitals. *Interactive Journal of Medical Research*, 1(2), e11. <http://dx.doi.org/10.2196/ijmr.2137>. PMID:23611956.
- Lee, S. M., Lee, D., & Schniederjans, M. J. (2011). Supply chain innovation and organizational performance in the healthcare industry. *International Journal of Operations & Production Management*, 31(11), 1193-1214.
- Luciano, E. M., Bragança, C. E. B., & Testa, M. G. (2011). Privacidade de informações de pacientes de instituições de saúde: a percepção de profissionais da área de saúde. *Revista Reuna*, 16(2), 1-14.
- Magnagnagno, O. A. (2015). *Mecanismos de proteção da privacidade das informações de prontuário eletrônico de pacientes de instituições de saúde* (Dissertação de mestrado). Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre.
- Magnagnagno, O. A., Luciano, E. M., & Britto-Da-Silva, V. R. (2015). Mecanismos para Proteção da Privacidade das Informações do Prontuário Eletrônico de Pacientes de Instituições de Saúde. In *Anais do XXXIX ENANPAD*. Brasil: ENANPAD.
- Marciano, J. L. P. (2006). *Segurança da Informação: uma abordagem social* (Tese de doutorado). Universidade de Brasília, Brasília.
- Min, H., & Zhou, G. (2002). Supply chain modeling: past, present and future. *Computers & Industrial Engineering*, 43(1-2), 231-249. [http://dx.doi.org/10.1016/S0360-8352\(02\)00066-9](http://dx.doi.org/10.1016/S0360-8352(02)00066-9).
- Patel, S. C., Graham, J. H., & Ralston, P. A. S. (2008). Quantitatively assessing the vulnerability of critical information systems: a new method for evaluating security enhancements. *International Journal of Information Management*, 28(6), 483-491. <http://dx.doi.org/10.1016/j.ijinfomgt.2008.01.009>.
- Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 70-82. <http://dx.doi.org/10.1016/j.cose.2015.10.006>.
- Sampieri, R. H., Collado, C. F., & Lucio, M. P. B. (2013). *Metodologia de pesquisa*. 5 ed. Porto Alegre: Penso.
- Samy, G. N., Ahmad, R., & Ismail, Z. (2010). Security threats categories in healthcare information systems. *Health Informatics Journal*, 16(3), 201-209. <http://dx.doi.org/10.1177/1460458210377468>. PMID:20889850.
- Song, F., Zhou, Y.-T., Wang, Y., Zhao, T.-M., You, I., & Zhang, H.-K. (2019). Smart collaborative distribution for privacy enhancement in moving target defense. *Information Sciences*, 479, 593-606. <http://dx.doi.org/10.1016/j.ins.2018.06.002>.
- Supply Chain Council – SCC. (2010). *Supply Chain Operations Reference (SCOR) model*. Texas.
- Ten, C.-W., Liu, C.-C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *Power Systems, IEEE Transactions on*, 23(4), 1836-1846. <http://dx.doi.org/10.1109/TPWRS.2008.2002298>.
- Warren, M., & Hutchinson, W. (2000). Cyber attacks against supply chain management systems: a short note. *International Journal of Physical Distribution & Logistics Management*, 30(7/8), 710-716. <http://dx.doi.org/10.1108/09600030010346521>.

- Wieser, P. (2011). From health logistics to health supply chain management. *Supply Chain Forum: An International Journal*, 12(1), 4-13.  
<http://dx.doi.org/10.1080/16258312.2011.11517249>.
- Zafar, H., & Clark, J. G. (2009). Current state of information security research in IS. *Communications of the Association for Information Systems*, 24(34), 557-596.  
<http://dx.doi.org/10.17705/1CAIS.02434>.