

Profiling IT Security and Interoperability in Brazilian Health Organisations From a Business Perspective


Rui Rijo, Polytechnic Institute of Leiria, Leiria, Portugal

Ricardo Martinho, Polytechnic Institute of Leiria & CINTESIS, University of Porto, Porto, Portugal

Adicinéia Aparecida Oliveira, Federal University of Sergipe, São Cristóvão, Brazil


Domingos Alves, Ribeirão Preto Medical School, University of São Paulo, Ribeirão Preto, Brazil

Zilma Silveira Nogueira Reis, Federal University of Minas Gerais, Belo Horizonte, Brazil

 <https://orcid.org/0000-0001-6374-9295>


Cátia Santos-Pereira, HLTSYS – HealthySystems, Porto, Portugal

Manuel E. Correia, DCC/FCUP, CRACS/INESC TEC, University of Porto, Porto Portugal

 <https://orcid.org/0000-0002-2348-8075>

Luís Filipe Antunes, CRACS INESC-TEC & FCUP & fHLTSYS, Porto Portugal

Ricardo João Cruz-Correia, CINTESIS, University of Porto, Porto Portugal

 <https://orcid.org/0000-0002-3764-5158>

ABSTRACT

The proliferation of electronic health (e-Health) initiatives in Brazil over the last 2 decades has resulted in a considerable fragmentation within health information technology (IT), with a strong political interference. The problem regarding this issue became twofold: 1) there are considerable flaws regarding interoperability and security involving patient data; and 2) it is difficult even for an experienced company to enter the Brazilian health IT market. In this article, the authors aim to assess the current state of IT interoperability and security in hospitals in Brazil and evaluate the best business strategy for an IT company to enter this difficult but very promising health IT market. A face-to-face questionnaire was conducted among 11 hospital units to assess their current status regarding IT interoperability and security aspects. Global Brazilian socio-economic data was also collected, and helped to not only identify areas of investment regarding health IT security and interoperability, but also to derive a business strategy, composed out of recommendations listed in the paper.

KEYWORDS

Business Perspective, Data Security, Health Informatics, Interoperability, Questionnaire

DOI: 10.4018/IJEHMC.2020040106

This article, originally published under IGI Global's copyright on April 1, 2020 will proceed with publication as an Open Access article starting on January 25, 2021 in the gold Open Access journal, International Journal of E-Health and Medical Communications (converted to gold Open Access January 1, 2021), and will be distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

INTRODUCTION

The use of Information Technologies (IT) and Information Systems (IS) in healthcare organizations has since long taken a very distinctive route. Business processes conducted in this particular area are different and specific to these working environments (Reichert, 2011). Particular needs include not only security and privacy measures regarding patient health information, but also interoperability needs and standards that only apply to the healthcare sector. Take, for instance, the special security rules around the Health Insurance Portability and Accountability Act (HIPAA) (Asfaw, 2008), or the Health Level 7 (HL7) standard developed purposely for the exchange, integration, sharing, and retrieval of electronic health information (Health Level Seven International, 2015). Other recent developments also include new security standards and interoperability approaches for instance, for pregnancy care (Moreira, Rodrigues, Sangaiah, Al-Muhtadi, & Korotaev, 2018), Internet of Things (IoT) scenarios (Bujari, Furini, Mandreoli, Martoglia, Montangero, & Ronzani, 2018).

Nevertheless, the healthcare sector still suffers from the lack of worldwide secure and interoperable IT and IS (Braunstein, 2018), with most efforts directed to the automation of daily routines within hospitals and overall health organizations (Moraes & Gómez, 2007; Venkatesh, Zhang, & Sykes, 2011).

In developing countries, this is aggravated by several socio-economic indicators, such as general poor health status, rampant diseases such as HIV/AIDS, and inadequate health services and policies (Davison, Harris, Qureshi, Vogel, & de Vreede, 2005; Braa, Hanseth, Heywood, Mohammed, & Shaw, 2007). Although Health Information Systems (HIS) are seen as crucial to reducing these problems (AbouZahr & Boerma, 2005), in practice issues like organizational complexity (Gladwin, Dixon, & Wilson, 2003) and fragmented and uncoordinated organizational structures, all contribute to a highly fragmented landscape where each organization ends up maintaining their own HIS (Chilundo & Aanestad, 2005).

This fragmentation is also the case in Brazil. While the use of IT in health organizations is widespread among most federal states and the access to information is a right granted by the Brazilian Federal Constitution, most citizens are not allowed to access their health records and transmit them digitally (Fornazin & Joia, 2016).

Current research studies also lack, in the authors' point of view, an important business perspective, i.e., the perspective of a company with skills and experience in implementing health IT, with a fair knowledge of a certain country's health IT share market, and with the purpose of becoming a new market entrant regarding Michael Porter's five competitive forces (Porter, 1979).

In this paper, the authors performed an exploratory case study involving 11 hospital units to perceive the status of HIS security and interoperability. These issues are amongst the greatest concerns of the interviewed Chief Information Officers. Additionally, the authors of this paper formed a consortium, where academia and industry knowledge/skills gathered around well-established research methods, to perform a market study on the business status of health IT in Brazil.

A real private company (hereafter, referred as "the company") was also part of the consortium, where its main health IT skills, interests and work capacity were considered for this study. Therefore, this business perspective takes not only from a focused profiling on the current use/implementation of concrete health IT technologies (in which this company excels) in Brazilian hospital units, but also on a macro economic and business analysis made up from data available in the World Bank database and empirical knowledge from the consortium.

Consequently, the research method is heavily influenced by two main drivers: 1) the academia members of the consortium proposing adequate health IT characterization methods such as questionnaires, interviews, statistical data analyses and market research; and 2) the industry and company members providing field experience and knowledge from a business perspective, to add value to decision makers wanting to become players in the Brazilian health IT market.

This paper is organized as follows: the next section refers background work on the characterization of health IT in developed and developing countries, particularly in Brazil. The authors then describe

the methods used to perform the profiling study, and present and discuss the obtained results from the field work. Crossing information from the questionnaire used, and from business data collected and experience knowledge derived in a business strategy proposed also in this section. The authors present the main limitations and conclusions of this study in the last section.

BACKGROUND

In the past decade, several research studies were conducted regarding the characterization of health IT and Health Information Systems (HIS) targeting developing countries. Important contributions (Braa, Hanseth, Heywood, Mohammed, & Shaw, 2007; Sæbø, Kossi, Titlestad, Tohouri, & Braa, 2011; Soar, Gow, & Caniogo, 2012; Kimaro & Nhampossa, 2007) have their focus specifically on the success/failure factors surrounding the efforts of implementing HIS and HIS-related policies and strategies. Conclusions drawn by Braa, Hanseth, Heywood, Mohammed, & Shaw (2007) led to a growing need of having integrated health information infrastructure based on common standards for information sharing and exchange between information systems, programs, and institutions.

Braga (2005) refers to an important political statement regarding HIS in Brazil: HIS created a proficuous research and market areas, where several political and financial interests began to be disputed.

In Brazil, there can be observed a diverse number of HIS, including, for instance, birth control systems, mortality information systems, socioeconomic information systems, information systems for disease control - tuberculosis, AIDS and hepatitis (Comissão Nacional de Energia Nuclear, 2010).

Security and interoperability concerns and measures in health IT and general healthcare information systems have been increasingly taking relevance in society over the last couple of years. This was encouraged by the General Data Protection Regulation (GDPR) enforcement in Europe from May 2018, bringing health IT security awareness not only to hospitals, but also to all stakeholders regarding health information such as patients, health IT suppliers, laboratories, research centers and medical schools (Spencer & Patel, 2019).

The need for this awareness motivated Kuo (2018) to realize a study correlating users of Electronic Medical Records Systems (EMRS) with their level of knowledge on information security management policies, and concluded that a successful EMRS adoption depends on this knowledge. The same study states that, since an EMRS is usually integrated with many other health information systems, the implementation of this interoperability should also be subjected to the information security management policies in charge.

Following this line, another recent study from Entzeridou, Markopoulou, & Mollaki (2018) revealed that the major concern of patients and physicians regarding EMRS is patient's information security and privacy. From a more technical point of view, Madhavi & Lincke (2018) assessed security risks in EMRS from the USA and concluded that most significant and costly security breaches included hacking, unauthorized access, theft, loss and improper disposal of health information.

On another revealing study presented by Kisekka & Giboney (2018), the authors found that increased privacy concerns affect the use of health records, the attitude towards interoperability and health information exchange, and even perceived care quality. On the other hand, trust in the effectiveness of information security increases the frequency of patient access to health records and positive attitude towards information exchange. In fact, Shaw, McGregor, Brunner, Keep, Janssen, & Barnet (2017) also correlate the effective use of health IT with improved care coordination, enhanced communication between providers and patients, and increased effectiveness in various measures of quality outcomes and provider performance.

Concrete technical surveying of health IT in the healthcare sector have been rehearsed by several case studies worldwide, including developed countries (DesRoches et al., 2008), developing countries (Tomasi, Facchini, & Maia, 2004), and also particularly in Brazil, including the ones belonging to the GESITI project, such as the works of Balloni (2011) and Oliveira et al. (2014). These studies

help to show the lack of adoption of interoperability and integration technologies, which contribute to the significant number of inconsistencies in information, preventing an effective understanding of the Brazilian population's health (Moraes & Gómez, 2007; Moraes, 1994).

Moreover, Moraes and Gómez (2007) sustained that this situation serves the interests of the state apparatus and of private businesses that wish to maintain the status quo of informational practices in health (Fornazin & Joia, 2016). This leads to the need of analysing Brazil's health IT market also from a business perspective, together with a sound analysis on security and interoperability issues that currently mostly concern health IT Chief Information Officers.

METHODS

This article draws heavily on the field study data collected from the health IT questionnaires and interviews conducted throughout 11 hospitals in Brazil. It also counts with the consortium's previous experiences in dealing with health business processes (Martinho, Rijo, & Nunes, 2015), enterprise architectures (Rijo, Martinho, & Ermida, 2015), effective use of health information standards (Ferreira, Carvalho, Gonçalves, & Correia, 2015), EHRs (Reis, Correia, & Pereira, 2011) and from characterizing IT in hospitals (Martinho, Varajão, Cunha, & Balloni, 2014).

Following a statistical analysis of the data thus collected, the authors worked on the business perspective, considering the following actions:

- Collection from the World Bank Open Data (The World Bank, 2018) of the main indexes regarding Brazil, namely GDP (and % invested in health), population, health IT investments forecasts, health market growth and number of hospitals;
- Business environment, namely human capital, IT infrastructure, digital education, and main challenges for making business in Brazil (including an interview with a Portuguese business man who had already established 3 companies in Brazil).

From this data and statistical analysis, several business strategy recommendations are proposed for a company willing to invest in Brazil.

Criteria to Choose Target Health Organizations for the Questionnaire

The choice of the target health organizations was drawn considering the following main criteria:

- **Management model:** Including 2 public NHS hospitals, 1 NHS hospital with private management, 2 University hospitals and 6 private hospitals;
- **Size:** Including 3 small-sized hospitals (up to 150 beds), 5 medium-sized (up to 500 beds) and 3 big capacity hospitals (more than 500 beds);
- **Location:** Considering the variety of state dimensions and economical and social realities. Sergipe, Bahia, Minas Gerais and São Paulo were the states chosen. Sergipe is the smallest Brazilian state while Bahia is the most touristic one. Minas Gerais is the third richest and one of the biggest, while São Paulo is the financial capital of Brazil.

Data Collection Methods

Data was collected through structured interviews to the CIOs in service at the hospitals visited, during the second quarter of 2017. The 11 structured interviews were carefully planned and executed for two months. Each interview was conducted face-to-face, considering a questionnaire with sixteen sections. The considerable size of the questionnaire and the need of providing adequate context for some of the questions, led us to opt for face-to-face interviews.

To further enhance the quality of the collected data, a static (PDF format) version of the questionnaire was previously emailed to each interviewee. Detailed data such as the size of the hospital, number of collaborators, number of hardware equipment and IT investment could then be previously collected by the CIOs in conjunction with other boards of the visited hospitals.

After each interview, the data collected was registered in a web application supporting an online version of the questionnaire, to be further exported for statistical analyses.

These analyses are depicted in a type of (template) chart showing the number of hospital units implementing and not implementing a certain measure, according to the used questionnaire.

Applied Questionnaire

The questionnaire used in the scheduled structured interviews was previously evolved, refined and tested with Brazilian and Portuguese stakeholders, reaching a final version number 5.4.

An online smaller version was made available after these structured face-to-face interviews, to be disseminated among the main health information systems associations in Brazil and Portugal, focusing on the expertise areas of the proposing company, namely HIS security, interoperability and standards. Thus, this smaller online version allowed the authors to disseminate the questionnaire in a more effective manner throughout other hospital units. Also, and since this online version was developed after the interviews in Brazil, it also allowed for a centralized and digital registration point of all the obtained results, and for exporting these for further comparisons and statistical analyses.

Table 1 summarizes the 16 sections of the questionnaire used, including the purpose of each section, the number of questions and the main data collection methods used.

Table 1. Summary of the 16 sections that composed the applied questionnaire

| Section | Purpose (Questions) | Collection Method |
|---------|--|-----------------------|
| 1 | Overview explanation of the questionnaire and terms of use | Face-to-face + Online |
| 2 | Hospital profile (name, address, website, number of beds, nurses, doctors, staff...) | Face-to-face + Online |
| 3 | Responder profile (name, age, background, position...) | Face-to-face + Online |
| 4 | IT Security (69 questions) | Face-to-face + Online |
| 5 | IT Interoperability (16 questions) | Face-to-face + Online |
| 6 | Hardware infrastructure (20 questions) | Face-to-face |
| 7 | Network infrastructure (10 questions) | Face-to-face |
| 8 | Existing Information Systems (15 questions) | Face-to-face |
| 9 | Business Process Management / Business Intelligence / Software development technologies (18 questions) | Face-to-face |
| 10 | Use of standards/taxonomies (11 questions) | Face-to-face |
| 11 | Use of quality (ISO) standards/certifications (8 questions) | Face-to-face |
| 12 | Research & Development activities (3 questions) | Face-to-face |
| 13 | IT Team profile (12 questions) | Face-to-face |
| 14 | Health Information Systems alignment with strategy (11 questions) | Face-to-face |
| 15 | Decision making and IT procurement processes (15 questions) | Face-to-face |
| 16 | IT investments in the past and priorities for the future (30 questions) | Face-to-face |

As it would be cumbersome presenting a detailed statistical analysis regarding all these sections in the form of a journal article, the authors focused this paper on the analyses of the above mentioned HIS security and interoperability measures.

RESULTS AND DISCUSSION

This section summarizes the results obtained from the 11 hospitals surveyed, focusing on the answers to sections 4 and 5 regarding security and interoperability measures taken by each hospital. It also addresses the business data collected regarding the Brazilian overall and specific health IT contexts, and concludes by presenting a business strategy for new health IT market entrants.

Summary on the Results of the Questionnaire

Below are presented condensed results obtained from the questionnaire regarding the current status on security and interoperability measures implemented across the 11 hospital units.

Security Measures

Figure 1 shows the overall number of security measures implemented by each of the 11 hospital units visited.

From all security measures surveyed, results are quite disparate within the 11 units, and range from about 42% of implemented measures (29 out of 69) in hospital h6, to 4 hospitals above 80% (h2, h5, h8 and h9). The average is around 73% of the security measures implemented (50.18 measures out of 69).

Figure 2 presents, for each surveyed measure, the number of hospitals implementing that measure (in blue) vs the number of hospitals not implementing (orange). It can be observed that 2 measures are fully implemented by all hospitals (Synchronized clock and Network addresses assigned in a structured manner), while the less implemented measure is There are rules for the duration of tests and the installing of security patches. Nevertheless, the average of implemented security measures within this group is 9.7 out of 14.

Regarding physical security, it can be observed in Figure 3 that the measure *The servers are located in an isolated area with access control* is fully implemented by all hospitals, while the measure that foresees the UPS software installation to automatically turn on/off servers is the least

Figure 1. Percentage of security measures implemented vs non-implemented for the 11 hospitals visited

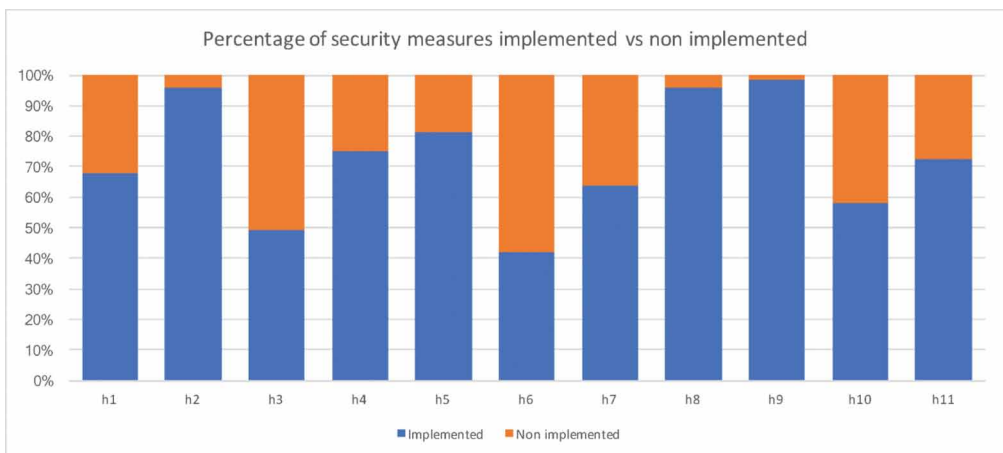


Figure 2. General security: Number of implemented vs non-implemented measures

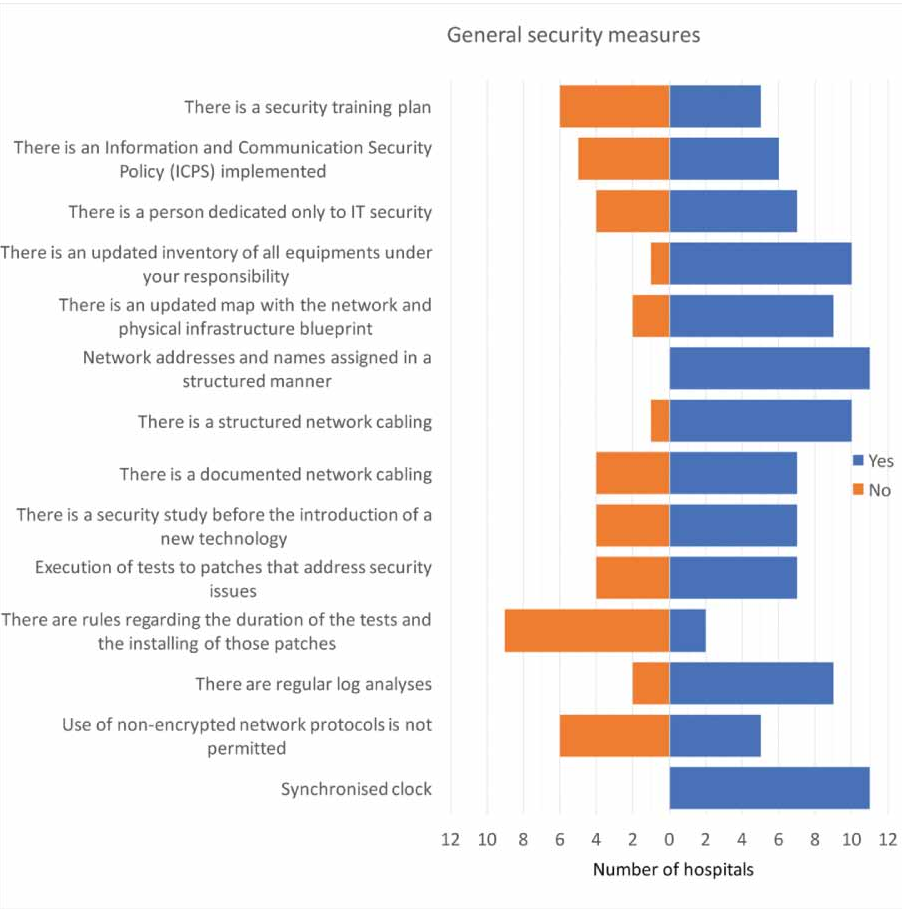
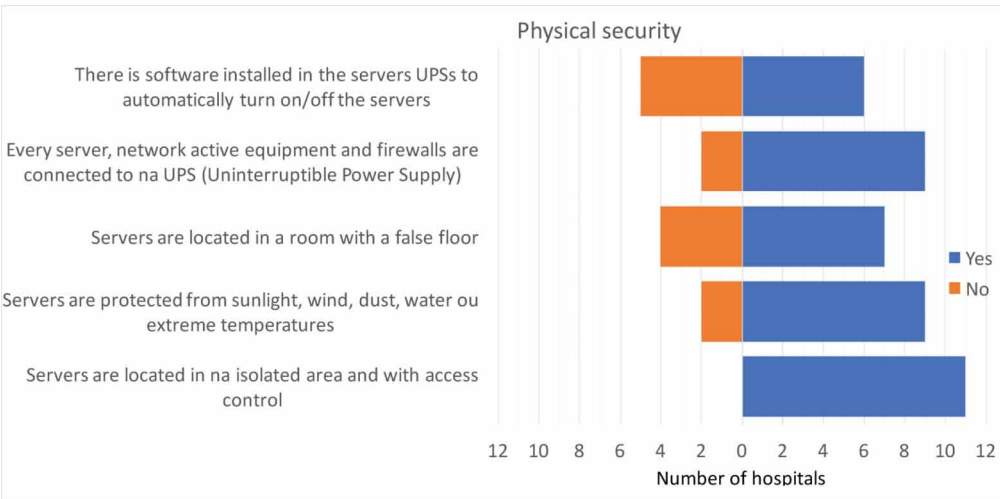


Figure 3. Physical security: Number of implemented vs non-implemented measures



implemented (6 out of 11 hospitals). This group also presents an average above 50% of implemented measures (3.8 out of 5).

For user and password management, there is also a positive outcome regarding the number of implemented security measures, with an average of 6.18 out of 9. Figure 4 shows that the measure all default passwords are immediately changed in every equipment is also fully implemented, while the measure preventing the use of the same passwords is the least implemented (only 5 out of 11 hospitals).

Intrusion detection and information privacy were also some of the measures assessed. As observed in Figure 5, the least implemented measure is the one that foresees privacy mechanisms when using e-mail to send health/medical information. All 9 of the 11 hospitals that use email to send this kind of information do not implement any security measure regarding privacy.

The security measure most implemented in this group is the resetting of passwords when using remote desktop sessions for support services by suppliers (10 out of 11). The average of implemented measures is, within this group, of 4.2 out of 7.

Regarding the surveyed questions about vulnerability security measures, and along with web security, this section is the one with the least average of implemented measures (5.2 out of 12).

Figure 6 shows measures that are not implemented in 7, 8 or even 10 hospitals, which reveals a wide unfamiliarity with most of these measures. Most implemented ones are the execution of at least one vulnerability test and the use of network traffic analysing tools.

Somehow in the opposite way of the previous section, issues related with virus and spam security measures are among the most implemented ones, as shown in Figure 7.

Anti-virus systems exist in all surveyed hospitals, while SPAMbots detection is only implemented in 4 hospitals. Average is 6.55 out of 10 implemented security measures in this group.

Security in Accessing Web Applications

As mentioned before, this is one of the least scored security group, as the 3 measures surveyed are not implemented in most of the hospitals (see Figure 8), with a low average of only 0.6 out of 3 measures implemented.

Figure 4. User and password management: Number of implemented vs non-implemented measures

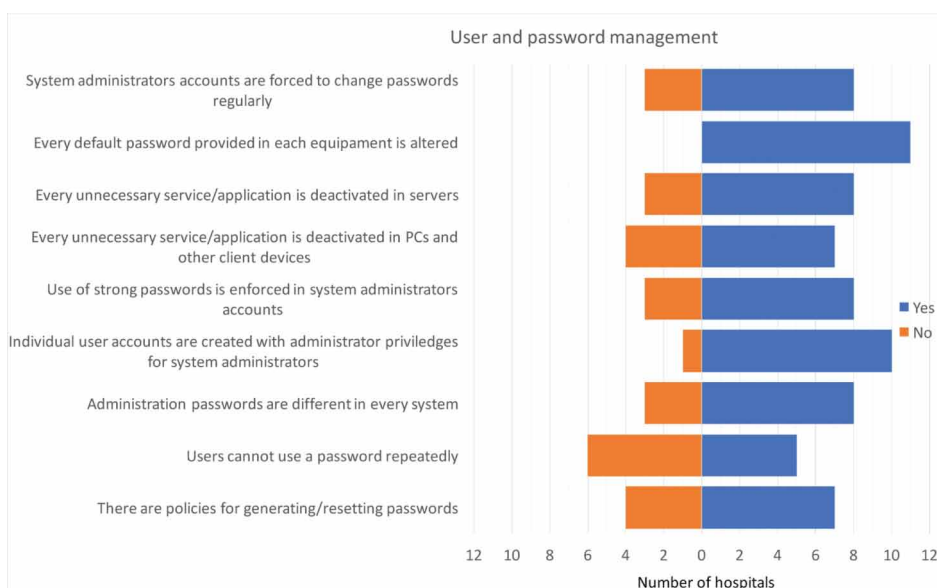


Figure 5. Internal and external infrastructures and security threats: Number of implemented vs non implemented measures

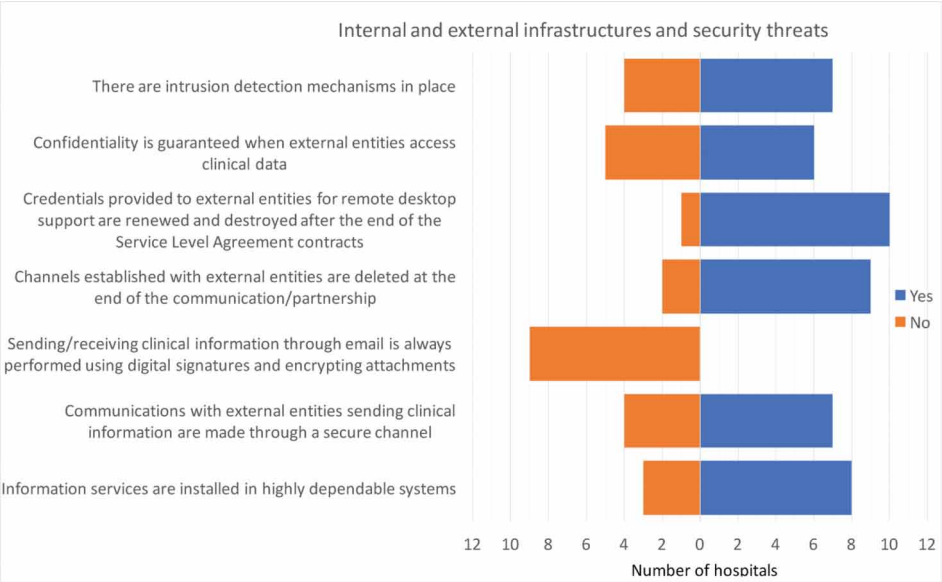


Figure 6. Security vulnerabilities and intrusion tests: Number of implemented vs non-implemented measures

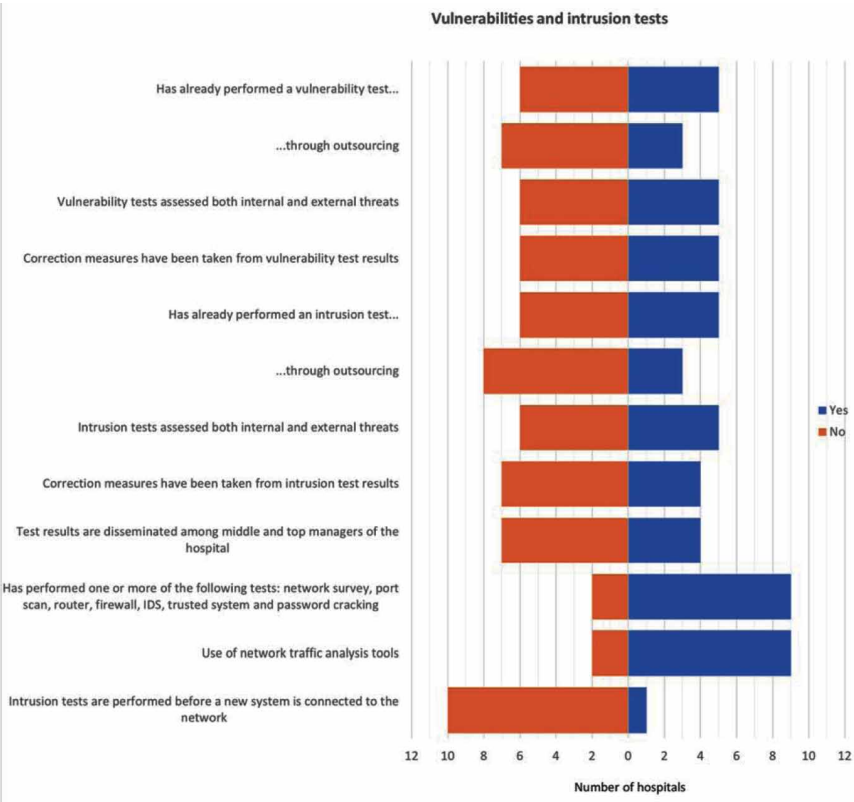


Figure 7. Virus/ Spam security measures: Number of implemented vs non-implemented measures

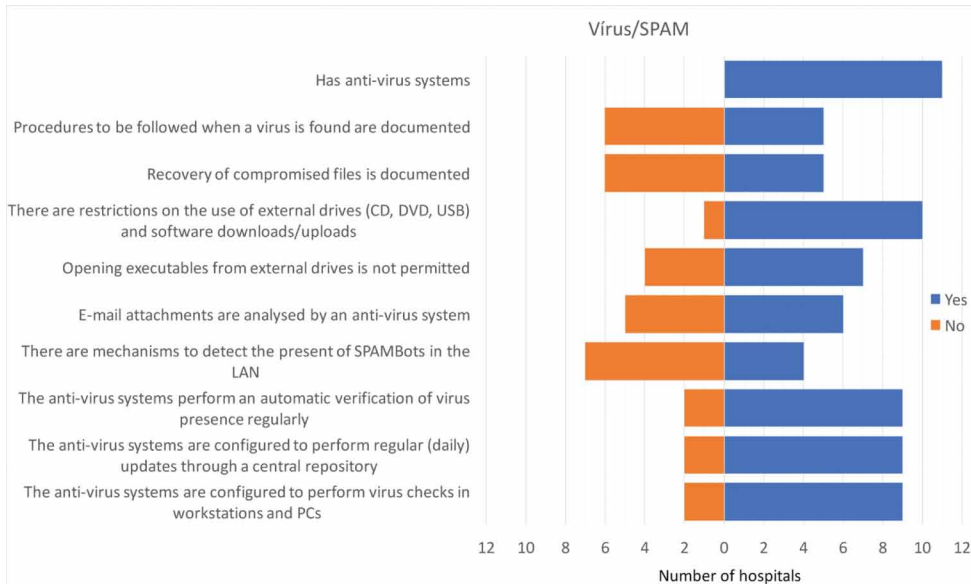
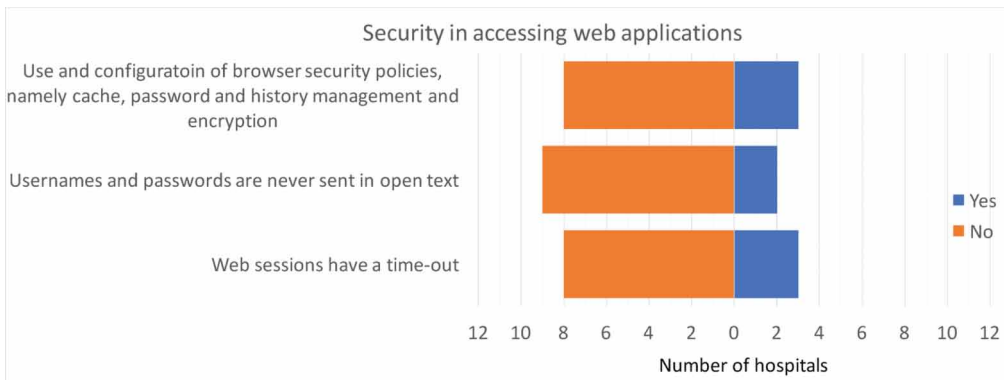


Figure 8. Security in accessing web applications: Number of implemented vs non-implemented measures



The existence of backups and the capacity of restoring data due to some incident is, in a general way, foreseen in every hospital, as can be observed in Figure 9. All hospitals do backups regularly, and almost all (9 out of 11) have rehearsed failures and data restoration procedures through backups. There is, however, a general unfamiliarity regarding renovation and technological updates in the media used for security copies. The average in this group is 3.7 out of 5 measures implemented.

Interoperability Measures

Figure 10 profiles interoperability measures implemented and non-implemented throughout the 11 surveyed hospitals. Overall, it can be observed that the main interoperability standards regarding health information are the ones presenting lower adoption. This is the case of HL7, with only 4 implementing HL7 2.x versions and 2 implementing HL7 3.x.

Figure 9. Backup/Restore: Number of implemented vs non-implemented measures

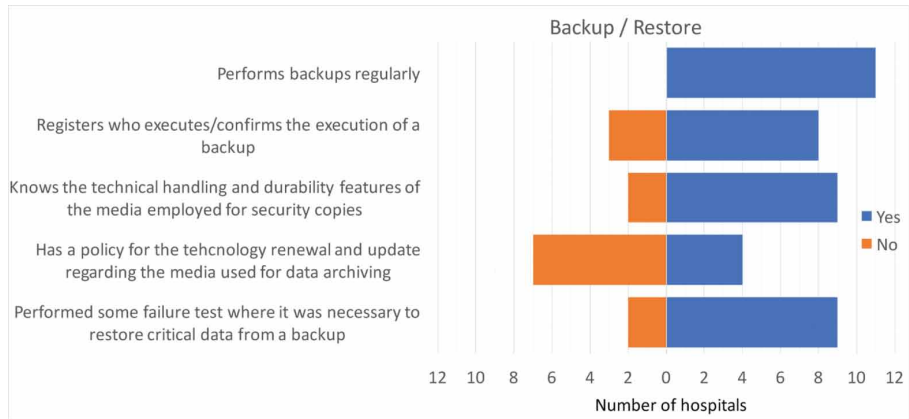
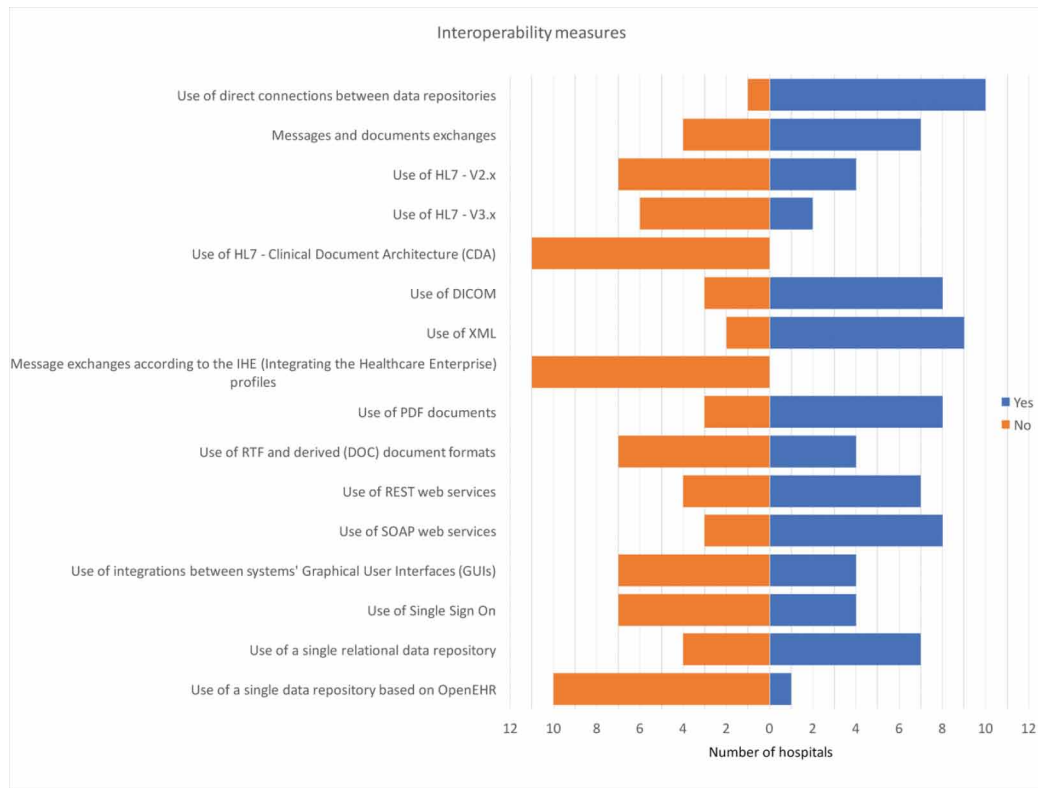


Figure 10. Interoperability measures: Number of implemented vs non-implemented measures



Regarding the HL7 Clinical Data Architecture (CDA) and the use of Integrating the Healthcare Enterprise (IHE) standards and guidelines to exchange messages and data between HIS, none of the hospital units surveyed has them implemented.

Other standard with a lower rate of adoption is OpenEHR (although strongly recommended and even regulated by the Brazilian government and health information systems' associations). Here, only

1 hospital has it implemented. This section presents also one of the lowest implementation averages of 5.4 out of 16.

There is, although, higher rates of adoption when it comes to the use of web service technologies (SOAP and REST) or basic interoperability technologies such as XML. Here, the majority of the hospital units use them especially to consume external (governmental) provided web services to report expenses and refundable resources. This is still, although, a very unidirectional communication from inside the hospital to external services.

As to internal interoperability, there is still a considerable number of hospitals that prefer using direct data integrations through Database Management Systems (DBMS).

Table 2 presents a summary on the scores obtained from the questionnaire made face-to-face with IT managers in all visited hospitals.

From these results, it can be clearly identified serious pitfalls regarding 2 groups of security measures: 1) vulnerabilities; and 2) accessing web applications. Here, the average of implemented measures is below 50% (less than half of the measures foreseen in the questionnaire), being of 20% in the case of the security configurations in accessing web applications.

Regarding the surveyed interoperability measures, it can be verified a wide unfamiliarity in what concerns the most advanced e-Health technologies. Here, HL7 implementation is still scarce, even considering the minor HL7 2.x versions (only 4 out of 11 hospitals). On the other hand, DICOM is

Table 2. Summary of results

| Section | More Impl. Measures (Number of Hospitals) | Less Impl. Measures (Number of Hospitals) | Average of Implemented Measures |
|-------------------------------------|---|--|---------------------------------|
| General security | 11 implemented Synchronized clock and Network addresses assigned in a structured manner | 2 implemented There are rules for the duration of tests and installing of security patches | 9.7 out of 14 |
| Physical security | 11 implemented The servers are located in an isolated area with access control | 6 implemented UPS software installation to automatically turn on/off servers | 3.8 out of 5 |
| User and password management | 11 implemented Every default password provided with equipment are altered | 5 implemented Prevent the use of the same passwords | 6.18 out of 9 |
| Internal and external threats | 10 implemented Reset passwords when using remote desktop for external support | 2 implemented Privacy mechanisms in email when sending medical information | 4.2 out of 7 |
| Security vulnerabilities | 9 implemented Intrusion security test tools and Network traffic analysers | 1 implemented Intrusion tests executed before switching new equipment onto the network | 5.2 out of 12 |
| Virus/SPAM | 11 implemented Anti-virus systems | 4 implemented SPAMbots detection | 6.55 out of 10 |
| Security accessing web applications | 3 implemented Browser configurations regarding cache, password and history encryption | 2 implemented Username and password credentials are never sent in free unencrypted text | 0.6 out of 3 |
| Backup/Restore | 11 implemented Backup and restore procedures | 4 implemented Renovation and technological updates in the media used for security copies | 3.7 out of 5 |

an exception here, mainly because it is a widespread practice to be implemented by vendors of RIS and PACS systems. Nevertheless, the predominant use of XML and SOAP interoperability measures also denotes the lack of maturity regarding a full integration of HIS and stored health information nation-wide. Even OpenEHR, which is a regulatory-based priority and should be faced as a basic technology for creating, storing and disseminating medical information between physicians and health professionals, is still only available to a few major hospitals.

Business Data

Table 3 summarizes some macroeconomic indexes regarding Brazil as to the year of 2017 (The World Bank, 2018), that are of interest to compose the business perspective.

Equally relevant are data that characterize the business environment. Table 4 shows most relevant information collected on this matter. Additional data collected included tax levels (about 68% from profit), loan rates (above 30% in 2015) and corruption level (notorious) (The World Bank, 2018).

To complement this kind of business data, the authors derived from their enterprise and industrial experience relevant information for a company who wishes to be a new market entrant.

Information collected from these experiences can be summarized as follows:

- Brazil is a market for companies with a high financial maturity level, that can endure some “starvation” before beginning to see the first benefits;
- Brazil and particularly São Paulo cost of life is high, of about 5 times more than Lisbon (reference city for the company);
- Labour laws are to be followed by the book. People do not have much social supports, so labour-related lawsuits filed by employees happen every day;
- It is always easy to go in with a local partner, although it is best to take cautions in the choice;
- Fiscal laws are complex, and justice is expensive and takes some time. Taxes over raw materials is legislated, but are unadjusted to the reality of IT companies;
- Customers often demand an upfront fee and go in for a shared revenues model, although after some time of proven benefits, this model can be changed, and companies can really have large incomes.

Table 3. Macroeconomic data collected about Brazil (Source: The World Bank (2018))

| | |
|--|---|
| GDP | 1 794 \$USD Billion (9th) |
| Population | 207 652 865 (5th) |
| GDP % for health | 9.6% |
| Health IT market forecast | 700 \$USD Million |
| Apps market forecast | 50 \$USD Million |
| Growth forecast in the private health market | 7.6% between 2016-2020 |
| Number of hospitals | 7 806 hospitals (21% do not have agreements with the NHS) |

Table 4. Business environment data

| | |
|--|---|
| Human capital | Low rate of IT graduates. Deficit of 200 000 IT technicians in 2017 |
| Overall IT and network infrastructure | Low coverage of WAN. Speed ranked in 67 th |
| Internet access | 41% of population with access to Internet (64 th) |
| Business environment | 121 st in “easy to make business” ranking |

The authors could observe that, although Brazil presents an enormous business potential, new market entrants have serious initial pressure, and must endure some time without visible benefits. They should even foresee a significant investment capacity with a long payback period, and partnerships with local companies are recommended, although risky. Large company customers have the power to demand upfront fees and negotiate shared revenues.

Proposed Business Strategy

From the results presented in the sections above, the authors derived the following business strategy (Table 5), including recommendations for a company willing to enter the health IT Brazilian market, specifically as a solution supplier for health IT security and interoperability.

CONCLUSION

In this paper, the authors present a combined technical/statistical and business perspective to tackle the lack of health IT security and interoperability measures, observed from 11 Brazilian hospitals. This perspective arose from the interdisciplinary consortium gathered for this study and included also a company with business interest in this market.

The company's professionals used their experience and skills to collaborate with academics and HIS associations from Brazil and Portugal, and to derive a data collection method based on a customized questionnaire and face-to-face interviews. The authors also took into consideration market share data regarding management policies, size and location of health organizations in Brazil.

The main contributions on this paper include an assessment on health IT security and interoperability on Brazilian hospitals, taking into consideration a sample of 11 hospital units. These units have been distinguished upon their management model, size and location, in order to provide a varied perspective of health IT through different kinds of hospitals. Although the number of surveyed

Table 5. Business environment data

| | |
|---------------------------------|--|
| Known facts | <ul style="list-style-type: none"> • Health IT in Brazil created proficuous research and business areas, where several political and financial interests began to be disputed; • The lack of adoption of interoperability and integration technologies contributed to a significant number of inconsistencies in health information, preventing an effective understanding of the Brazilian population's health; • This situation serves the interests of the state apparatus and of private businesses that wish to maintain the status quo of informational practices in health; • There is a need of analysing Brazil's health IT market also from a business perspective, together with an analysis on IT security and interoperability issues that currently mostly affect health organizations. |
| Proposed recommendations | <ul style="list-style-type: none"> • Health IT interoperability can be a medium-to-long term investment in Brazil, since the overall health IT customers (both public and private hospitals) are still to find value in these kinds of solutions; • Health IT security can be an easier market to explore in the short-term, since there is nowadays a great concern on these issues, and an equally great demand for specialized suppliers; • From side observations noted during the hospital visits and interviews, it was also perceived a business opportunity regarding health data anonymization services (some hospitals have the largest health databases in South America, which could be used by worldwide researchers if properly anonymized); • Public hospitals and the public national health sector should not be an investment priority for a private company. Small and medium-sized hospitals where IT managers have decision power should be the best segment to invest, since big hospitals tend to enforce high pressure on suppliers; • Interpersonal relationships are part of Brazil's business environment DNA, and exploring the contact network or partnering to reach decision makers should also be a priority. Having a local presence is essential to assure a fluid pre-sales, sales and support cycle, regarding the services provided. |

hospitals is a limitation of this study, the authors were able to confirm the obtained data with the knowledge derived from their long experience and curricula on the status of health IT in Brazil.

Another contribution includes a cross-study between these questionnaire results, World Bank economic data from Brazil and information retrieved from the authors' business experience, deriving in a set of recommendations for companies wishing to enter the Brazilian health IT market.

On these recommendations, the authors could conclude that the lack of wide implementation measures related with intrusion detection and configuration of web access policies constitute an explorable market opportunity in the short-term. Similarly, the experience in implementing and training professionals regarding the main interoperability standards HL7, CDA and integration engines such as Mirth and HealthConnect can also contribute to a company's differentiation in the Brazilian health IT panorama, regarding medium-to-long term investments.

ACKNOWLEDGMENT

The authors would like to thank all technical and medical staff from the 11 hospital units surveyed, and all their efforts to gather the requested data for this study. This research was supported by the São Paulo Research Foundation (FAPESP) [Process number 2018/00307-2].

REFERENCES

- AbouZahr, C., & Boerma, T. (2005). Health information systems: The foundations of public health. *Bulletin of the World Health Organization*, 83, 578–583. PMID:16184276
- Asfaw, E. (2008). *Health insurance portability and accountability act (HIPAA): Confidentiality and privacy from the perspectives of the consumer and the physician*. Capella University.
- Balloni, A. J. (2011). *Projeto GESITI Hospitalar: uma avaliação da GEstão em SIstemas e Tecnologias de Informação em Hospitais*. Campinas, SP: CTI/MCT.
- Braa, J., Hanseth, O., Heywood, A., Mohammed, W., & Shaw, V. (2007). Developing health information systems in developing countries: The flexible standards strategy. *Management Information Systems Quarterly*, 31(2), 381–402. doi:10.2307/25148796
- Braga, P. D. (2005). Política, tecnologia e informação em saúde: A utopia da emancipação. *Revista de Administração Contemporânea*, 9(1), 246–246. doi:10.1590/S1415-65522005000100018
- Braunstein, M. L. (2018). Health Care in the Age of Interoperability: The Potential and Challenges. *IEEE Pulse*, 9(5), 34–36. doi:10.1109/MPUL.2018.2856941 PMID:30273142
- Bujari, A., Furini, M., Mandreoli, F., Martoglia, R., Montangero, M., & Ronzani, D. (2018). Standards, security and business models: Key challenges for the IoT scenario. *Mobile Networks and Applications*, 23(1), 147–154. doi:10.1007/s11036-017-0835-8
- Chilundo, B., & Aanestad, M. (2004). Negotiating multiple rationalities in the process of integrating the information systems of disease-specific health programmes. *The Electronic Journal on Information Systems in Developing Countries*, 20(1), 1–28. doi:10.1002/j.1681-4835.2004.tb00129.x
- Comissão Nacional de Energia Nuclear. (2010). Plano Diretor de Tecnologia da Informação de 2010-13, Ministério da Saúde. Secretaria Executiva. Retrieved from http://www.cnem.gov.br/images/cnem/documentos/publicacoes/PDTI_2010-2012.pdf
- Davison, R. M., Harris, R. W., Qureshi, S., Vogel, D. R., & de Vreede, G. J. (Eds.). (2005). *Information systems in developing countries: theory and practice*. City University of HK Press.
- de Oliveira, S. B., Nogueira, H. G. P., Villardi, B. Q., Olivares, G., de Schueler, A. S., & Balloni, A. J. (2014). Tecnologia da informação em hospitais públicos e universitários: Um diagnóstico em cinco hospitais da cidade do Rio de Janeiro. *GESITI*, 70058, 125.
- DesRoches, C. M., Campbell, E. G., Rao, S. R., Donelan, K., Ferris, T. G., Jha, A., & Blumenthal, D. et al. (2008). Electronic health records in ambulatory care—A national survey of physicians. *The New England Journal of Medicine*, 359(1), 50–60. doi:10.1056/NEJMsa0802005 PMID:18565855
- Ferreira, R. J. T., Correia, M. E. C. D., Gonçalves, F. N. R., & Correia, R. J. C. (2015, June). Data Quality in HL7 Messages--A Real Case Analysis. In *Proceedings of IEEE 28th International Symposium on Computer-Based Medical Systems (CBMS)*, São Carlos and Ribeirão Preto - Brazil: IEEE. doi:10.1109/CBMS.2015.30
- Fornazin, M., & Joia, L. A. (2016). Linking theoretical perspectives to analyze health information and communication technologies in Brazil. *Government Information Quarterly*, 33(2), 358–368. doi:10.1016/j.giq.2016.04.004
- Gladwin, J., Dixon, R. A., & Wilson, T. D. (2003). Implementing a new health management information system in Uganda. *Health Policy and Planning*, 18(2), 214–224. doi:10.1093/heapol/czg026 PMID:12740326
- Health Level Seven International. (2015). HL7 Standards Product Brief - HL7 Version 3 Product Suite. Retrieved from http://www.hl7.org/implement/standards/product_brief.cfm?product_id=186
- Kimaro, H., & Nhampossa, J. (2007). The challenges of sustainability of health information systems in developing countries: Comparative case studies of Mozambique and Tanzania. *Journal of Health Informatics in Developing Countries*, 1(1), 1–10.
- Kuo, R. Z. (2018). EMRS Adoption: Exploring the effects of information security management awareness and perceived service quality. *Health Policy and Technology*, 7(4), 365–373. doi:10.1016/j.hlpt.2018.10.012

Madhavi, A., & Lincke, S. (2018). Security Risk Assessment in Electronic Health Record System. In *Proceedings of the 2018 IEEE Technology and Engineering Management Conference (TEMSCON)*. Evanston, IL USA: IEEE. doi:10.1109/TEMSCON.2018.8488449

Martinho, R., Rijo, R., & Nunes, A. (2015). Complexity analysis of a business process automation: Case study on a healthcare organization. *Procedia Computer Science*, 64, 1226–1231. doi:10.1016/j.procs.2015.08.510

Martinho, R., Varajão, J., Cunha, M. M. C., & Balloni, A. (2014). Tecnologias e sistemas de informação em entidades hospitalares: dois casos de hospitais portugueses. In Balloni, A. J., Levy, S. N., Nemer, et al. (Eds). *Por que GESITI?: Gestão de Sistemas e Tecnologias da Informação em Hospitais: panorama, tendências e perspectivas em saúde*. Campinas-SP, Ministério da Saúde - DATASUS.

Moraes, I. H. S. D. (1994). *Informações em saúde: da prática fragmentada ao exercício da cidadania*. São Paulo, Brazil: HUCITEC.

Moraes, I. H. S. D., & Gómez, M. N. G. D. (2007). Informação e informática em saúde: Caleidoscópio contemporâneo da saúde. *Ciencia & Saude Coletiva*, 12(3), 553–565. doi:10.1590/S1413-81232007000300002 PMID:17680109

Moreira, M. W., Rodrigues, J. J., Sangaiah, A. K., Al-Muhtadi, J., & Korotaev, V. (2018). Semantic interoperability and pattern classification for a service-oriented architecture in pregnancy care. *Future Generation Computer Systems*, 89, 137–147. doi:10.1016/j.future.2018.04.031

Porter, M. E. (1979). How competitive forces shape strategy. *Harvard Business Review*, 21–38. PMID:18271320

Reichert, M. (2011). What BPM technology can do for healthcare process support. In *Proceedings of the Conference on Artificial Intelligence in Medicine in Europe*. Pavia, Italy: Springer, Berlin, Heidelberg. doi:10.1007/978-3-642-22218-4_2

Reis, Z. S. N., Correia, R. J. C., & Pereira, A. D. C. (2011). Electronic information systems for women's health care, teaching and research: A plea for an higher involvement of health professionals? *Revista Brasileira de Ginecologia e Obstetrícia*, 33(3), 107–110. PMID:21829993

Rijo, R., Martinho, R., & Ermida, D. (2015). Developing an Enterprise Architecture proof of concept in a Portuguese hospital. *Procedia Computer Science*, 64, 1217–1225. doi:10.1016/j.procs.2015.08.511

Sæbø, J. I., Kossi, E. K., Titlestad, O. H., Tohouri, R. R., & Braa, J. (2011). Comparing strategies to integrate health information systems following a data warehouse approach in four countries. *Information Technology for Development*, 17(1), 42–60. doi:10.1080/02681102.2010.511702

Shaw, T., McGregor, D., Brunner, M., Keep, M., Janssen, A., & Barnet, S. (2017). What is eHealth (6)? Development of a conceptual model for eHealth: Qualitative study with key informants. *Journal of Medical Internet Research*, 19(10), e324. doi:10.2196/jmir.8106 PMID:29066429

Soar, J., Gow, J., & Caniogo, V. (2012). Sustainability of health information systems in developing countries: The case of Fiji. *The HIM Journal*, 41(3), 13–19. doi:10.1177/183335831204100302 PMID:23087079

Spencer, A., & Patel, S. (2019). Applying the Data Protection Act 2018 and General Data Protection Regulation principles in healthcare settings. *Nursing Management*, 26(1). Retrieved from <https://journals.rcni.com/nursing-management/cpd/applying-the-data-protection-act-2018-and-general-data-protection-regulation-principles-in-healthcare-settings-nm.2019.e1806/print/abs>

The World Bank. (2018). World Bank Open Data. Retrieved from <http://data.worldbank.org/>

Tomasi, E., Facchini, L. A., & Maia, M. D. F. S. (2004). Health information technology in primary health care in developing countries: A literature review. *Bulletin of the World Health Organization*, 82, 867–874. PMID:15640923

Venkatesh, V., Zhang, X., & Sykes, T. A. (2011). “Doctors do too little technology”: A longitudinal field study of an electronic healthcare system implementation. *Information Systems Research*, 22(3), 523–546. doi:10.1287/isre.1110.0383

Rui Rijo is Professor of Computer Science at the Polytechnic Institute of Leiria. He received his PhD in Computer Science from the Trás-os-Montes University and his Engineering degree from Instituto Superior Técnico (Technical University of Lisbon). He has more than ten years of experience as senior information systems consultant in, among other countries, Tokyo (Japan), Macau (China), Hong-Kong (China), São Paulo (Brazil), Kuala Lumpur (Malaysia), Madrid (Spain), Amsterdam (Holland), Madrid (Spain) and Lisbon (Portugal). His publications include book chapters and papers in refereed national and international conferences and journals. He was the general chair of HCist - International Conference on Health and Social Care Information Systems and Technologies and associate editor of the International Journal of Web Portals and editor of the International Journal of E-Health and Medical Communications. He was the dean of the Healthcare Informatics course and currently is the dean of the Master on Healthcare Information Systems Management. His is also Pesquisador Visitante Especial (PVE-CSF/CAPES, process number: 88881.068176/2014-01) at Universidade de São Paulo (USP) with the project "Healthcare software evaluation from the perspective of the relation between the patient and health professionals". His current research interests include project management, software engineer, and health information systems.

Ricardo Martinho is an Associate Professor at the School of Technology and Management – Polytechnic Institute of Leiria, Portugal. He teaches several subjects related to enterprise information systems, enterprise application development, software engineering (agile methods) and healthcare computer programming and information systems. He graduated in Electrical Engineering – Computer Science at University of Coimbra, received his MSc in Computer Science - Information Systems Programming from IST - Technical University of Lisbon, and his PhD from University of Trás-os-Montes and Alto Douro. He is currently the Head of the Healthcare Informatics BSc. degree, and participates as a consultant in several enterprise and health informatics-related research projects. He supervises several MSc and PhD theses in the Computer Science – Health Informatics research areas. He has several publications in conference proceedings, book chapters and journals, related to the Business Process Management, Software Engineering and health informatics research areas. He serves as editor-in-chief, member of editorial board and reviewer for several books and international journals, and has served in several committees of international conferences. He is a co-founder of HCist – International Conference on Health and Social Care Information Systems and Technologies (<http://hcist.scika.org>)

Domingos Alves is currently associate professor in the Department of Social Medicine at the Medical School of Ribeirão Preto, USP. He is leader of the Laboratory of Health Intelligence (LIS). Acting mainly in the following areas: Theoretical and Computational Modeling in Health, Simulation of Health Services and Health Information Systems.

Zilma Silveira Nogueira Reis is the coordinator of the Health Informatics Centre in the Faculty of Medicine (UFMG), since 2012. Vice-president of the Brazilian Society of Health Informatics (SBIS). Awardee in the 14th. Round of Grand Challenges Explorations of the Bill & Melinda Gates Foundation (2015). Awardee in the 9th Round of Grand Challenges Canada, Stars in Global Health (2018). The team Newborn Skin-age was selected for Building Global Innovation Program by ISCTE-IUL - MIT, 7th Edition, 2016 and Venture Well (2017). Visitant professor at Lisbon University (2018-2019). I am experienced in Maternal and Child Health, and Medical Informatics, acting on the following topics: medical informatics, scientific methodology, and women's health.

Cátia Santos - Pereira has a MSc degree in Medical Informatics and a MSc degree in Services Engineering and Management. Currently she is PhD student of Engineering and Industrial Management Doctoral Program in University of Porto and in healthy systems responsible for product planning. Has experience in computer security specially applied in healthcare environment, product planning and design and project management.

Manuel Eduardo Correia has a PhD in Computer Science from the University of Porto and a MSc in Computer Engineering from Imperial College. He is a Professor at the computer science department of the Faculty of Science, where he was director of the master's course on computer security from 2014 until 2018. He is currently the Pro-Rector responsible for digital infrastructures at the University of Porto. He has an extensive experience in national and international computer security research projects at the CRACS group of INESC TEC Porto, where he has worked extensively in the field of anomaly detection and identity management. He has also been a technical advisor for some Portuguese public agencies (Health and Education), namely acting as a consultant for the security of the national electronic prescription system, being also responsible for the development of the biometric match-on-card system, currently being deployed by the Portuguese national citizen (eID) card.

Luís Filipe Coelho Antunes, Full Professor of the Computer Science Department at Faculty of Sciences, University of Porto (FCUP). Director of the Competence Centre for Cybersecurity and Privacy, University of Oporto. Senior researcher at INESC.Tec. Member of the Scientific Council of FCUP and member of the Council for Electronic Administration at the University of Porto. Develops research activity in the field of computer security has several scientific publications, successfully guided 5 PhD students and belongs to several research projects funded by FCT. Has exercised consultancy activity in the area of computer security for the Ministry of Health and the Portuguesa Data Protection Commission, is accredited by the National Security Cabinet and is expert in ENISA (European Union Agency for Network and Information Security) in the area of eID and eGovernment eHealth. Luís Antunes appears regularly on TV program as information security expert. In 2013 co-founded a spin-off from the University, called HealthySystems that centers its activity in the area of information security with a strong focus on auditing, eID and anonymization techniques. Recently co-founded the University of Porto spin-off Adyta. Adyta main objective is to promote specialized security solutions tailored to the needs of sovereign bodies dealing with sensitive or classified information and large business groups Adyta focuses its activity in the defense field and securing communications through innovative solutions and adjusted to each customer. This spin-off is the result of several years of collaboration with the Portuguese National Security Agency. Also founder of the start-up TekPrivacy (www.tekprivacy.pt) that leveraging on his vast experience in privacy and data protection aims to develop solutions to assist the work of the data protection officer.

Ricardo João Cruz-Correia is an Auxiliary Professor at the Faculty of Medicine of University of Porto (FMUP). In 1996 achieved the degree of Computer Science at the Faculty of Sciences (FCUP), in 1998 achieved a master's degree on Computer Science also at FCUP, and achieved the PhD at FMUP in 2008 on the Integration of Hospital Information Systems. Has nearly 200 scientific articles in health informatics. He has collaborated on the implementation of several health information systems. Member of several health informatics standard organizations (HL7, openEHR, IPQ CT199, ABNT Brasil), and associations (APIM, e-MAIS). He has lectured several disciplines on Medical Informatics (e.g. "Health Information Systems and Electronic Patient Records", "Models of clinical information and health integration standards") of pre and pos graduation courses, and is currently supervising several PhD and Master thesis on Health Informatics. Co-founder of 3 UP spin-off companies (www.hltsys.pt, www.virtualcare.pt, www.is4health.com) and a professional school (www.ciencia-letras.pt).