Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022)
Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, and Simon Wilson
©2022 ESREL2022 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-5183-4_R11-03-651-cd

Assessing Risk Awareness with Hospital Information Systems

Margarida Martins

University of Coimbra, CISUC, DEI, Portugal. E-mail: mdmartins@student.dei.uc.pt

João Barata

University of Coimbra, CISUC, DEI, Portugal. E-mail: barata@dei.uc.pt

Noel Carroll

J.E. Cairnes School of Business & Economics, NUI Galway, Ireland. E-mail: noel.carroll@nuigalway.ie

Hospital information systems continue to transform healthcare practices at a disruptive rate. However, such transformational changes within healthcare practices also introduce new technical risks. Therefore, all stakeholders within a healthcare setting must be aware of the potential risks hospital information systems pose to patient care safety and quality. This paper adopts a focus group study and Delphi method approach to examine (i) the range of risks identified by thirty-two experts from different Portuguese hospitals and (ii) the level of awareness across healthcare practitioners. The contribution of the research is threefold. First, we present a literature summary on risks associated with hospital information systems. Second, we present findings on a typology of twenty-three risks and evaluate the perception of healthcare professionals on their potential impacts. Third, we discuss strategies to improve risk awareness with hospital information systems within the hospital environment, with broader implications for other healthcare settings, considering the different perspectives of healthcare workers.

Keywords: Risk awareness, Hospital digital transformation, Hospital information systems, Risk identification, Risk analysis, Risk typology.

1. Introduction

Hospital information systems (HIS) are designed to manage healthcare data, supporting various needs such as administrative tasks or clinical decision-making. Therefore, HIS are essential to improving healthcare services' safety and quality (Salahuddin et al., 2020). Moreover, the rapid evolution of information technologies (IT) and the digitalization of patient data require more efficient technical requirements, particularly in communications, architecture, security, and system response time (Farzandipour et al. 2020).

Healthcare information systems provide the tools to ensure hospital stakeholders access critical information such as vital records, financial status, and security information (Carroll et al. 2016). Therefore, preventing "*errors that could impose harm to patients within the care process from using the HIS*" (Salahuddin et al. 2020) has become a priority worldwide.

Modern risk assessment plans must include a risk identification guide, risk typology analysis, and a mitigation plan (Haghighi and Torabi, 2020). Information systems are no exception, and there are essential studies revealing security threats (e.g., power failure) (Samy et al. 2010), business continuity frameworks (Haghighi and Torabi, 2020), and the increasing privacy concerns (Park and Shin 2020). However, there has been a growing focus on risk during the COVID-19 pandemic and more frequent reports of cybersecurity attacks. This poses new challenges for hospitals, confirmed by the significant healthcare service impacts of the Conti Ransomware attack on the Health Service Executive (HSE), the national healthcare provider in Ireland. Recent literature reviews reveal the difficulties in risk identification and awareness in "hospital silos", suggesting "*creative ways of continual training and approaches to awareness of the healthcare sector urge security and privacy* *practitioners in hospitals to ensure continuous awareness to bring about a culture change*" (Ahouanmenou, Van Looy, and Poels 2022).

Our contribution to HIS risk-awareness literature focuses on identifying 23 risks within the hospital environment, evaluating stakeholders' awareness, and suggesting potential improvements.

This research commenced with a comprehensive literature review. In addition, we interviewed research participants within hospital risk offices, progressing with focus groups and a Delphi panel to detail the findings.

The remainder of the paper is structured as follows. Section 2 presents a literature review on HIS risks and some knowledge gaps. Section 3 describes the research methods. Section 4 explains the main findings, followed by the discussion. Finally, Section 5 summarizes the main conclusions, limitations, and future work opportunities.

2. Literature Review

Risk identification is critical in information systems adoption (e.g., software, hardware, social implications, networks, data, etc.) and is mandatory in healthcare contexts (Haghighi and Torabi 2020). Risk assessment is a key part of risk management which aims to identify organizational weaknesses and implement required actions. In addition, risk assessment can support organizations to audit processes and improve the overall quality of the service while complying with quality standards and assuring organization accreditation—for example, the ACSA accreditation model (Almuedo-Paz et al. 2012).

Several authors have proposed risk analysis approaches in healthcare institutions. For example, Septian and Pamuji (2019) work for information security management to ensure national and ISO standards compliance. Their study shows the benefits of effective communication between hospital management and IT departments.

HIS risks must be addressed by both clinical and IT departments. An example of a study on HIS risk identification used a fuzzy matrix to define the overall impact of every risk identified (Haghighi and Torabi, 2020). The authors separate HIS risks into five components: software, hardware, human, network, and database/data warehouse, with 31 risks identified. Despite the importance of this example, the authors analyze a single institution. Nowadays, the risk typology continues to evolve rapidly, mainly due to the new challenges; for example: "*[c]ybersecurity threats are estimated to cost the world US $6 trillion a year by 2021, and the number of attacks has increased five-fold after COVID-19*" (Williams et al. 2020). In addition, Sheikh et al. (2021) studied the impact of the COVID-19 pandemic on the United Kingdom (UK) National Health Systems, revealing the amount of pressure the system was suffering and the remarkable advances in digital transformation. The main concerns on HIS were prioritized while describing the long-term plan for UK's digital transformation, namely (Sheikh et al. 2021):

1. Top-down/bottom-up adoption of IT that focuses on integrating infrastructure for hosting, storage, networks, and cyber security while simultaneously encouraging the involvement of local healthcare providers.
2. Close collaboration between developers, healthcare staff, and patients to achieve usability and interoperability.
3. Handling, processing, and analyzing data to be integrated into different systems, increasing interoperability by developing ethical frameworks and regulatory settings for data governance.
4. Addressing security and privacy concerns by encouraging employees to engage in security information training and providing mechanisms for patients to access their own data.

5. Fostering digital inclusivity by teaching those who might have lower levels of digital literacy (Kuek and Hakkennes 2020) how to connect with the hospital stakeholders digitally (e.g., colleagues, patients, third-party entities).

HIS risk awareness among healthcare professionals is a significant concern in the healthcare sector, mainly regarding how to store, export, and share sensitive data without creating possible HIS data breaches. On the one hand, data is exponentially increasing. Therefore, additional regulations such as the General Data Protection Regulation (GDPR) are ensured data protection and prevent confidentiality breaches. On the other hand, data protection measures are more complex. For example, electronic health records (EHR) de-identification techniques using chained hashing to generate short-lived pseudonyms and, therefore, reduce the impact of inference attacks (Rai 2022) require more technical knowledge from healthcare professionals.

Human aspects of HIS risks should evolve side-by-side with technical advances. Shah (2020) points to informatics teaching within the medical curriculum. Earlier studies, such as an online survey conducted by Walpole et al. (2017) across 34 UK medical schools, aimed to understand the extension of training in health informatics and bring awareness to medical educators of the importance of this subject. Despite the growth in health informatics teaching, nearly one-third answered "no" to the question *'on graduation, do students feel confident to use informatics in their role as doctors?'*. Studies concur on the shortcomings of health informatics skills in the undergraduate medical curriculum (Shah 2020; Walpole, Taylor, and Banerjee 2017). Moreover, these studies highlight that health informatics is scarcely assessed, and the course content is outdated, showing a substantial variation in content and teaching methods. However, the postgraduate scenario does not differ significantly. According to Jidkov et al. (2019), clinicians' health informatics competencies in the UK training curriculum are inadequate, fragmented, and suboptimal. They might imply that hospital information systems knowledge is underrated, despite the straightforward evidence that health informatics training improves the success of digital implementation. Jidkov et al. (2019) suggest adding 20 competencies to the pre-existing medical curriculum aimed at (1) information governance and security-focused procedures, (2) system use and clinician safety to control the EHR and electronic prescriptions, as well as encourage hardware familiarity. Collaborating in simulated clinical learning environments, e.g., university-simulated clinical skills laboratories, can also provide a valuable resource to support students develop technical competencies as they graduate into a digital healthcare environment (Carroll et al. 2018).

Digital communication is an optimal competency that ensures the protection of patient data sharing and security while tackling the "work from home" and remote data management. Patient empowerment is also necessary to adopt health informatics, ensuring patients have the necessary information to manage their health independently and facilitating medical practitioners in their daily work (Jidkov et al. 2019).

In many cases, healthcare providers can lack knowledge of current HIS security threats. For example, it was reported that the lack of knowledge of information security (HSE 2021) was a leading cause of the Conti cyber-attack on the Irish Health Services Executive (HSE) on 14 May 2021. The HSE report (HSE 2021) concluded that critical information was only periodically backed up to offline tape. Large data segments can be unrecoverable if an attacker does not provide the decryption codes. Moreover, information about applications was not recorded and up to date in a central or offline application database within the HSE. They also relied heavily on specific individuals, which led to a slow response time (US Department of Health & Human Services 2022). It is crucial to learn from missed opportunities and (1) identify the priorities; (2) develop new or improved risk assessment frameworks; and (3) implement more effective audit processes.

The literature provides substantial evidence that HIS risk awareness among healthcare professionals is critical; must be mandatory; is required by standard hospital regulations (Almuedo-Paz et al. 2012); and should result from multidisciplinary approaches (Haghighi and Torabi 2020). Risk identification and awareness are critical in the initial stages of training (Shah 2020; Walpole, Taylor, and Banerjee 2017) and run-time phases of auditing, prevention, and continuous improvement (Almuedo-Paz et al. 2012). Moreover, it should be constantly updated because digital transformation and societal challenges are evolving at an accelerated pace (Sheikh et al. 2021).

Nevertheless, more studies on HIS risk awareness involving experts with different backgrounds and healthcare institutions are crucial.

3. Research methodology

The study adopts a dual research method. First, the focus group technique collected data about HIS risks. Focus groups are popular in social studies, promoting a group discussion on the topic selected by the researcher, an active participant in the session (Morgan 1996). A Delphi panel (Linstone and Turoff 1975) was then organized to analyze priorities found in the first stage.

The focus group progressed in four main steps: (i) research design, (ii) data collection, (iii) analysis, and (iv) reporting of results (Rabiee 2004). First, we selected a total of 32 participants with different backgrounds in healthcare practice: a group of doctors from the center and south region of Portugal, both from hospitals and primary healthcare centers, and a group of nurses from centered hospitals to pediatric care as well as pharmaceuticals employees, ranging in different age ranges, and both female and male.

The preparation included exploratory meetings with the risk office staff of a district hospital, concluding that it was interesting to start with a small list of five open survey questions:

(i) Which Hospital Information Systems do you use daily?

(ii) Do you usually encounter (or know about) difficulties when using these systems?

(iii) Have you ever participated in a quality audit?

(iv) In your opinion, state the significant risks when using HIS

(v) Which functionalities would you like to see implemented in the current HIS?

These survey questions determined the fundamental relation between the practitioners and the HIS they use daily.

The survey was available for one week. After analyzing the answers, a meeting was scheduled with various participants. The next stage was a crucial point whereby risks and quality assessment were defined and captured perception (i) from a medical practitioner’s perspective, and (ii) from a patient perspective. The extensive and diversified focus group provided insights from operational and support roles (e.g., finance, administration, medical care, patient care, reputation, and social interactions). Moreover, there were no power structures among the group members promoting a situation where they could freely express their concerns and positive and negative experiences within their organization.

4. Findings

After the initial assessment of their use of HIS daily, it was essential to determine how the practitioners perceived the risks associated with their use and therefore score them accordingly to clarify the level of awareness of HIS-related risks.

4.1. Identification of risks

The survey identified vital risk categories that emerged from the open discussion and were developed and shared. The average scoreboard was obtained on a scale from one to ten: one represented a negligible risk, and ten indicated the most critical risk (see Table 1).

Table 1. First risk assessment and their average risk score.

Risk	Avg. Risk Rating
Lack of interoperability between systems	10
Errors in the Electronic Health Record (EHR)	9
Lack of innovation	9
Poor software training	9
Medical practitioners well-being	9
Lack of user-friendly interfaces	9
Poor communication	8
Interns learning process	8
Pandemic scenarios (COVID-19)	8
Financial aspects not aimed at medical knowledge	8
System's dependencies	7
Non-compliance with laws and regulations	7
Lack of audits	7
Government measures instability	7
Cyber-security/ Data breached	7
Lack of knowledge	6
Unethical conduct by medical providers.	6
Loss of accreditation	6
Lack of organizational culture	6
Change in the hospital's administration	6
Hierarchy conflicts	6
Addition of a new HIS	5
Media Communication	3

When analyzing Table 1, it is essential to clarify that although the focus group largely comprised medical practitioners, the survey's results and the discussion were shared between all the professionals.

4.2 HIS Risk Awareness

Following the focus group after two rounds of surveys, the Delphi method discussed the results with a smaller group of experts (five doctors and one engineer as a facilitator). The experts were asked individually which points from the last focus group survey contributed to reducing the risks and achieving the overall quality of the service provided.

Data breach issues were viewed as one of the main topics to discuss, especially since the COVID-19 pandemic increased the practice of remote working, and practitioners in quarantine were asked to keep working from home. Lower scores were justified by practitioners that referred that "those risks did not implicate a system failure and were not noticeable". A discussion on the lower scores on some crucial risks was open, and a compilation of points of view was composed:

- **New HIS**: according to the experts participating at this stage, the addition of a new HIS does not constitute a significant risk because new and innovative systems are favorable, assuming that proper training is provided.
- **Media communications**: media communications did not threaten the system's quality of service. Private information about the organization can be exposed.
- **Hierarchy conflicts**: conflicts between different points of view will always exist since different generations tend to look at a problem from a different perspective.
- **Unethical conduct by medical providers**: in the rare occasions that this occurred, the overall quality of the systems was not altered.
- **Interns' learning process**: medical practitioners are always learning. The learning curve is initially prominent, but with time, it flattens but never disappears.
- **Lack of knowledge**: this risk does not bring concerns because interns rarely decide on important subjects independently.
- **Financial aspects**: sometimes, the financial board measures the number of procedures made, not the quality. However, to succeed, the practitioner is aware that the quality of the

service provided is irrefutable when pursuing a career in healthcare.

5. Discussion

The changes to the healthcare system require the proficiency and management of professionals with health informatics knowledge, management, leadership skills, clinical practice, and an understanding of the demands frontline clinicians face in healthcare services (Meredith et al., 2021).

After analyzing the results from the focus group and comparing the risks identified by Haghighi and Torabi (2020), the lack of awareness of informatics issues is evident. Given that the study participants had further education in HIS and healthcare management, it was expected that HIS-related risks were familiar to them. However, the lack of hardware management training was not identified as a risk. Moreover, the EHR errors raised by the practitioners were focused on human aspects (lack of system training), and small system failures were often misunderstood by the practitioners and idled until the IT department raised the issue. Risk awareness programs must be improved with HIS-related risks due to the increasing impact of technology on patient safety and healthcare quality.

The lack of interoperability between systems was identified as the most impactful risk because it is time-consuming to input data multiple times and susceptible to human error as it is a dreary process. Nevertheless, all the 23 risks identified in our study are relevant to be included in awareness programs.

Nine out of twenty-three (39%) risks identified were IT-related, namely, cyber-security (identified by 100% of the participants), error with EHR (30 of the 32), system's interoperability failures (28/32), interface issues (not user-friendly, dated, with 24/32), poor software training (19/32), lack of innovation (12/32), system's dependencies (7/32) insufficient IT audit procedures (7/32), and introduction of a new HIS (5/32).

According to the respondents, the pandemic changed the HIS risk landscape significantly, hospitals were forced to embark on eHealth quickly, and risk awareness was not a top priority. However, unexposed risks may compromise confidence in HIS adoption, requiring more effective risk awareness strategies to prevent a step back in eHealth.

The Delphi stage revealed some curious answers. For example, the low-risk perception in new HIS adoption reveals extreme confidence that "others" will take care of the necessary training (not the doctors' primary concern). Moreover, the doctor's perspective on media communication seems limited (e.g., misses the importance of information disclosure for patients), and the impact of unethical conduct seems low (perhaps because they are thinking about their behavior and not how the HIS should deal with prevention). In contrast, the optimistic view on the impact of interns' training is alarming.

Integrating risk awareness management in the role of a Chief Clinical Information Officer (CCIO) could be an interesting option to support the multistakeholder perspective of risk awareness. Current HIS risk-awareness responsibility is siloed in the IT department and the quality and risk management office. According to the literature's insights, confirmed during our contacts with practitioners, several communication barriers exist between IT and clinical staff.

On the one hand, technical risks (e.g., systems vulnerability, computer viruses, authentication permissions, data integrity) tend to dominate the daily concerns of IT departments. On the other hand, staff and patients are the primary focus of risk management offices, eventually compromising the continuous update in (highly dynamic) HIS risk plans. For example, some workarounds used by medical staff during minor system failures (e.g., using paper records and spreadsheets) may significantly impact patient data protection and integrity.

The awareness of HIS risks should be a result of a sociotechnical analysis. However, future research is necessary to compare the results of structural changes in HIS risk-awareness.

6. Conclusions and Future Research

This study showed that digital transformation in hospitals has a massive impact on how people perceive the quality of services. This research identified 23 HIS risks and its awareness of different healthcare professionals in the post-pandemic stage of healthcare. The findings reveal that new risk awareness strategies and training programs are necessary to ensure the safe and effective use of HIS.

There are also significant limitations that must be stated. First, the study included a relevant sample of healthcare staff from different institutions and professional backgrounds. It was essential to contrast perspectives, but the context is restricted to Portugal. National policies and specificities of national graduation programs may influence the findings. Second, the risk analysis represents priorities in the pandemic/post-pandemic stage. The enormous pressure on healthcare facilities, reducing some healthcare procedures (e.g., non-urgent surgery), and the administration priorities should be considered. Therefore, the findings are more relevant to understanding changes in moments of healthcare disruptions and extreme pressures. Third, focus groups and Delphi studies provide a qualitative analysis of the phenomena and allow direct contact with the practitioners, promoting discussions. Nevertheless, the sample did not represent all the country's healthcare professionals and did not include all the possible healthcare skills. Additional work may include a survey to detail differences among the professionals that we confirmed at this stage.

There are exciting opportunities for future research in risk awareness for HIS. First, a cross-national comparison between countries with a healthcare system can be conducted to understand how different countries deal with new challenges that the hospital’s digital transformation brings. Second, study the proposal of actions for each risk according to different professionals (clinical, IT, administrative, patients), contrasting the perspectives of different stakeholders.

Acknowledgement

This work was partially supported by national funds through the FCT – Foundation for Science and Technology, I.P., within the scope of the project CISUC-UID/CEC/00326/2020 and by European Social Fund, through the Regional Operational Program Centro 2020.

References

Ahouanmenou, Steve, Amy Van Looy, and Geert Poels. 2022. "Information Security and Privacy in Hospitals: A Literature Mapping and Review of Research Gaps." Informatics for Health and Social Care 00 (March): 1–17. https://doi.org/10.1080/17538157.2022.2049274.

Almuedo-Paz, A., D. Núñez-Garcia, V. Reyes-Alcázar, and A. Torres-Olivera. 2012. "The ACSA Accreditation Model: Self-Assessment as a Quality Improvement Tool." In Quality Assurance and Management, edited by Mehmet Savsar, 289–314. InTech.

Carroll, N., Travers, M., and Richardson, I. 2016. Connecting Multistakeholder Analysis Across Connected Health Solutions. In: International Joint Conference on Biomedical Engineering Systems and Technologies. Presented at: BIOSTEC'16; February 21-23, Rome, Italy.

Carroll, N., Richardson, I., Moloney, M., and O’Reilly, P. 2018. Bridging healthcare education and technology solution development through experiential innovation. Health and Technology, 8(4), 255-261. https://doi.org/10.1007/s12553-017-0209-z

Farzandipour, Mehrdad, Zahra Meidani, Ehsan Nabovati, Monireh Sadeqi Jabali, and Razieh Dehghan Banadaki. 2020. "Technical Requirements Framework of Hospital Information Systems: Design and Evaluation." BMC Medical Informatics and Decision Making 20 (1): 1–10. https://doi.org/10.1186/s12911-020-1076-5.

HSE. 2021. "Conti Cyber Attack on the HSE Independent Post Incident Review Commissioned by the HSE Board in Conjunction with the CEO and Executive Management Team." https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf.

Jidkov, Lydia, Matthew Alexander, Pippa Bark, John G. Williams, Jonathan Kay, Paul Taylor, Harry Hemingway, and Amitava Banerjee. 2019. "Health Informatics Competencies in Postgraduate Medical Education and Training in the UK: A Mixed Methods Study." BMJ Open 9 (3). https://doi.org/10.1136/bmjopen-2018-025460.

Kuek, Angeline, and Sharon Hakkennes. 2020. "Healthcare Staff Digital Literacy Levels and Their Attitudes towards Information Systems." Health Informatics Journal 26 (1): 592–612. https://doi.org/10.1177/1460458219839613.

Linstone, Harold A., and Murray Turoff. 1975. The Delphi Method: Techniques and Applications. Edited by M Linstone, H. A., & Turoff. Reading, MA.

Morgan, David L. 1996. "Focus Groups." Annual Review of Sociology 22 (1): 129–52. https://doi.org/10.1146/annurev.soc.22.1.129.

Motevali Haghighi, S., and S. Ali Torabi. 2020. "Business Continuity-Inspired Fuzzy Risk Assessment Framework for Hospital Information Systems." Enterprise Information Systems 14 (7): 1027–60. https://doi.org/10.1080/17517575.2019.1686657.

Narayana Samy, Ganthan, Rabiah Ahmad, and Zuraini Ismail. 2010. "Security Threats Categories in Healthcare Information Systems." Health Informatics Journal 16 (3): 201–9. https://doi.org/10.1177/1460458210377468.

Park, Yong Jin, and Donghee Shin. 2020. "Contextualizing Privacy on Health-Related Use of Information Technology." Computers in Human Behavior 105 (October 2019): 106204. https://doi.org/10.1016/j.chb.2019.106204.

Rabiee, Fatemeh. 2004. "Focus-Group Interview and Data Analysis." Proceedings of the Nutrition Society 63 (4): 655–60. https://doi.org/10.1079/pns2004399.

Rai, Bipin Kumar. 2022. "Ephemeral Pseudonym Based De-Identification System to Reduce Impact of Inference Attacks in Healthcare Information System." Health Services and Outcomes Research Methodology, no. 0123456789. https://doi.org/10.1007/s10742-021-00268-2.

Salahuddin, Lizawati, Zuraini Ismail, Raja Rina Raja Ikram, Ummi Rabaah Hashim, Ariff Idris, Nor Haslinda Ismail, Noor Hafizah Hassan, and Fiza Abdul Rahim. 2020. "Safe Use of Hospital Information Systems: An Evaluation Model Based on a Sociotechnical Perspective." Behaviour and Information Technology 39 (2): 188–212. https://doi.org/10.1080/0144929X.2019.1597164.

Septian, R. F., and G. C. Pamuji. 2019. "Risk Analysis of Dutch Healthcare Company Information System." In IOP Conference Series: Materials Science and Engineering, vol. 662, no. 2, p. 022041. IOP Publishing.

Shah, Sam. 2020. "Digital Health Leadership: Carving a New Pathway." Future Healthcare Journal 7 (3): 199–201. https://doi.org/10.7861/fhj.dig-2020-path.

Sheikh, Aziz, Michael Anderson, Sarah Albala, Barbara Casadei, Bryony Dean Franklin, Mike Richards, David Taylor, Holly Tibble, and Elias Mossialos. 2021. "Health Information Technology and Digital Innovation for National Learning Health and Care Systems." The Lancet Digital Health 3 (6): e383–96. https://doi.org/10.1016/S2589-7500(21)00005-4.

US Department of Health & Human Services. 2022. "Lessons Learned from the HSE Cyber Attack." https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf.

Walpole, Sarah, Paul Taylor, and Amitava Banerjee. 2017. "Health Informatics in UK Medical Education: An Online Survey of Current Practice." JRSM Open 8 (1): 205427041668267. https://doi.org/10.1177/2054270416682674.

Williams, Christina Meilee, Rahul Chaturvedi, and Krishnan Chakravarthy. 2020. "Cybersecurity Risks in a Pandemic." Journal of Medical Internet Research 22 (9): 7–10. https://doi.org/10.2196/23692.