Information Security and Privacy in Hospitals: A Literature Map and Review of Research Gaps

Steve Ahouanmenou[a]*, Amy Van Looy[a], Geert Poels[a, b]

[a]*Faculty of Economics and Business Administration, Department of Business Informatics and Operations Management, Ghent University, Ghent, Belgium*

[b]*FlandersMake@UGent – core lab CVAMO, Ghent, Belgium*

Steve Ahouanmenou is a PhD researcher in the Faculty of Economics and Business Administration, Ghent University, Belgium, and is currently Director in Information Security & Global Data Governance at BDO Global. His research interests include information security and privacy in the public sector from a management and organizational perspectives. Steve was awarded "Belgium 40under40 2021".

Amy Van Looy is an associate professor with the Faculty of Economics and Business Administration, Ghent University, Belgium, and is head of the research cluster "Process orientation" at the UGentMIS Management Information Systems research group. Her research interests include business process management and digital innovation. Amy is the recipient of the "Highest Award for Achievement" at the Dale Carnegie Consulting Program in 2007, the "Award for Best Contribution" at the OnTheMove Academy in 2010, and other paper rewards. She was nominated in the top-10 for "Young ICT Lady of the year 2014" by DataNews and was recognized as a tech role model by "InspiringFifty Belgium" in 2020.

Geert Poels is a senior full professor in Management Information Systems at the Faculty of Economics and Business Administration of Ghent University, Belgium. He directs the UGentMIS Management Information Systems research group of the Department of Business Informatics and Operations Management and coordinates within this group the Enterprise Modeling, Engineering and Architecture (EMEA) research cluster. He is also member of the CVAMO core lab of FlandersMake@UGent. His research interests include conceptual modelling, business process architecture, data protection and privacy, phishing, and service science. He also teaches, guides master dissertation research, and is a program board member of the Master in Enterprise Architecture organized by IC Institute – innocom company, Beerzel, Belgium.

Information Security and Privacy in Hospitals: A Literature Mapping and Review of Research Gaps

(a) Objective: Information security and privacy are matters of concern in every industry. The healthcare sector has lagged in terms of implementing cybersecurity measures. Therefore, hospitals are more exposed to cyber events due to the criticality of patient data. Currently, little is known about state-of-the-art research on information security and privacy in hospitals. The purpose of this study is to report the outcome of a systematic literature review on research about the application of information security and privacy in hospitals.

(b) Method: A systematic literature review following the PRISMA methodology was conducted. To reference our sample according to cybersecurity domains, we benchmarked each article against two cybersecurity frameworks: ISO 27001 Annex A and the NIST framework core.

(c) Results: Limited articles in our papers referred to the policies and compliance sections of ISO 27001. In addition, most of our sample is classified by the NIST function "Protect," meaning activities related to identity management, access control and data security. Furthermore, we have identified key domains where research in security and privacy are critical, such as big data, IOT, cloud computing, standards and regulations.

(d) Conclusion: The results indicate that although cybersecurity is a growing concern in hospitals, research is still weak in some areas. Considering the recrudescence of cyber-attacks in the healthcare sector, we call for more research in hospitals in specific managerial and non-technical domains of information security and privacy that are uncovered by our analysis.

Keywords: healthcare, cybersecurity, privacy, SLR, research agenda

1. Introduction

Information security and privacy in the healthcare sector are subjects of increasing significance. Digital patient records, increased regulation, vendor due diligence, cyber-attacks, and the increasing need for data sharing between patients and third parties demonstrate the need for security and privacy (Burns et al., 2016).

Previous academic studies have been conducted on how to protect the access and use of patient data (Aarestrup et al., 2020). For instance, one systematic literature review (SLR) on cybersecurity in the healthcare sector tackled US healthcare quality (Appari & Johnson, 2010). Another SLR on information security and privacy in hospitals focused on electronic health records (EHRs) systems (Fernández-Alemán et al., 2013). Other studies related to cybersecurity in hospitals offer cybersecurity models (Naconha, 2021) or highlight the problem from an organisational (Jalali & Kaiser, 2018) or risk-management angle (Argaw et al., 2020)

Although prior studies show interesting findings on information privacy and security in hospitals, the focus of these studies was not on identifying research gaps. Consequently, there is a lack of knowledge regarding state-of-the-art research on information security and privacy in hospitals.

To our knowledge, a dedicated analysis of the state of literature regarding information security and privacy practices in hospitals is missing. That is the reason this article is specifically aimed at identifying the cybersecurity areas relevant to hospitals where research has been the most predominant or has been lacking. In addition, the paper provides a comprehensive research agenda for further academic studies in information security and privacy in hospitals.

Considering the increase in cyber events targeting patient data (Muthuppalaniappan & Stevenson, 2021), the objective of our study is to answer the

research question (RQ): What is the state of research about information security and privacy in hospitals?

For this purpose, we conducted an SLR, which is typically intended to present a representative evaluation of a research topic by using a trustworthy, rigorous, and auditable methodology (Keele, 2007). Also, we use two cybersecurity frameworks: ISO/IEC 27001 and NIST. This enables us to benchmark best practices for cybersecurity and identify investigated domains. We also follow a clear and structured path to present a research agenda for future research.

Our study's main contribution is the provision of a comprehensive research agenda by mapping investigated areas in hospitals' cybersecurity landscape from the perspective of two cybersecurity frameworks.

In section 2, we proceed with the background to our research by presenting the study's underlying concepts and related frameworks. Then, we describe the SLR approach in section 3 before presenting the research results in section 4. We discuss the findings and draw conclusions in sections 5 and 6, respectively.

2. Research background

The term "hospital" defines an institution for the study of diseases and training of healthcare personnel, maintained for the management and treatment of people in need of medical attention (Finch, 1994).

To provide background to our RQ and define the scope of our study, we first define the concepts of cybersecurity and information security. Then, we define the concept of information privacy. Finally, we describe the practice-related frameworks for information security and privacy. We use these frameworks as a structure to classify the reviewed studies.

2.1. Definition of cybersecurity and information security

The term "cybersecurity" is still broadly used with a variety of definitions that are often not comprehensive (Craigen et al., 2014). The term is usually associated with a deep technical expertise in the area of information technology (IT), although its scope extends to all aspects of an organisation, namely information security, operational technology (OT) and privacy practices related to digital assets (Galinec et al., 2017).

Nonetheless, professionals in the field tend to agree that cybersecurity must be distinguished from physical security because cybersecurity encompasses every effort to protect information and technology from harm, caused accidentally or intentionally (Guiora, 2017).

However, information security and cybersecurity terms are intertwined because cybersecurity has yet to properly handle the soft issues of information security and fully recognize the technical nature of security (Kosseff, 2018). Therefore, we define information security as a continuous sense of assurance that information risks and applicable controls are in constant balance (Anderson, 2003). This definition caught our attention, since it highlights the element of risk as the main driver of information security.

2.2. Definition of information privacy

The current understanding of information privacy is difficult to grasp because it is fragmented and discipline-dependent (Dinev et al., 2013). In general, information privacy refers to individuals' desire to control or have some influence over data about themselves (Bélanger & Crossler, 2011).

When translated to our subject, hospitals have the obligation to protect patient data but face serious privacy challenges, namely purpose limitation, transparency and fairness in processing due to the amount of sensitive data collected (Correia et al., 2019).

Therefore, in Europe, The General Data Protection Regulation was implemented in May 2018 (Crutzen et al., 2019). In addition, to increase the regulatory constraints on hospitals, GDPR has prompted the effectiveness and harmonization of personal data protection (Shabani & Borry, 2018). Similar laws exist for other regions as well, albeit with their own particularities.

Our research background ranges from cybersecurity to privacy and includes all domains within these concepts, as illustrated in Figure 1.

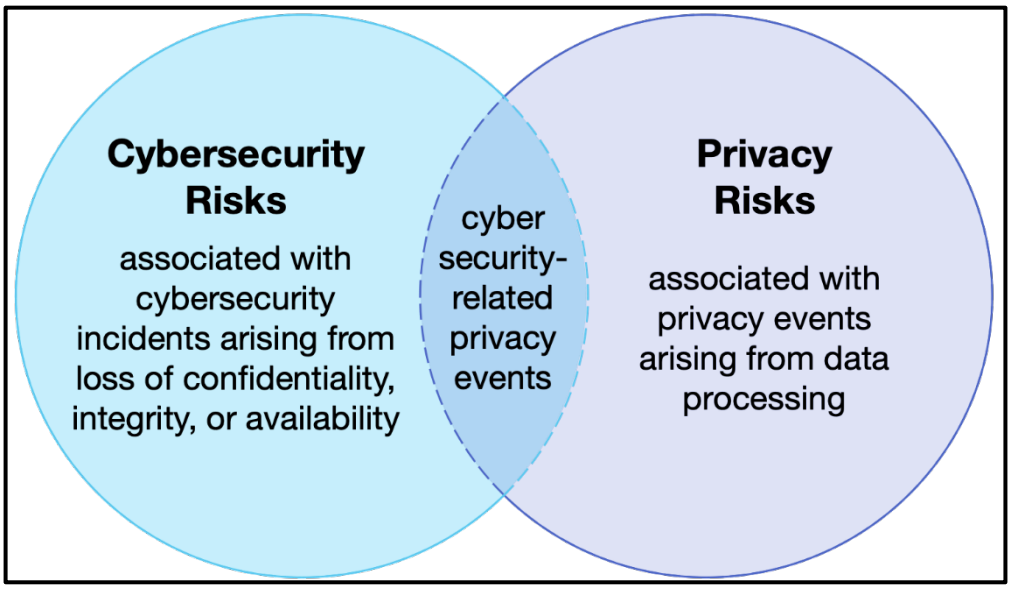

Figure 1: Cybersecurity and Privacy[1]

2.3. Cybersecurity best practices

The frontier between privacy and cybersecurity is narrow, with ever-increasing dependencies because of the digitalization of more data that could affect privacy (Sipior & Ward, 2001). Furthermore, the relation between cybersecurity and information security is complex and difficult to apprehend (Guiora, 2017).

[1] New to Framework | NIST

In response, the industry has developed methodologies to determine an integrated, consistent approach to tackle information security breaches and privacy invasions (NIST, 2013). We cover two established frameworks, namely the ISO 27001 Framework and the Cybersecurity Framework of the US National Institute of Standards and Technology (NIST). These frameworks are generic, as they do not assume a specific context of application, such as hospitals.

In our data analysis, these frameworks allow us to structure our classification of reviewed papers, e.g., to identify domains covered by these frameworks that are rarely addressed by the reviewed studies.

2.3.1. ISO/IEC 27001 Framework

ISO/IEC 27001 serves as our first framework to analyse our sample. ISO 27001 is an information security standard included in the ISO 27000 family that can be used as a guideline to develop and maintain an information security management system (ISMS) (ISO, 2013). ISO 27001 was most recently updated in 2017 (ISO/IEC 27001:2017). The standard comprises the information security requirements and a set of controls known as Annex A (Brenner, 2007) (Table 1). Annex A consists of 14 categories of security controls named clauses, with a total of 114 controls (Disterer, 2013). To achieve certification, organisations are expected to demonstrate that all the clauses are addressed.

Table 1: Annex A[2]

[2] ISO 27001: The 14 Control Sets of Annex A Explained (itgovernance.co.uk)

Clauses	Name	Number of controls
A.5	Information Security Policies	2
A.6	Organisation of Information Security	7
A.7	Human resource Security	6
A.8	Asset Management	10
A.9	Access Control	14
A.10	Cryptography	2
A.11	Physical and environmental security	15
A.12	Operations security	14
A.13	Communication Security	7
A.14	System acquisition, development, and maintenance	13
A.15	Supplier relationship	5
A.16	Information Security Incident management	7
A.17	Information Security aspects of business continuity management	4
A.18	Compliance	8

ISO 27001 Annex A will allow us to classify each article of our sample against the clauses.

The NIST Cybersecurity Framework

Secondly, we describe the NIST Cybersecurity Framework. The US NIST provides guidelines in various domains to achieve an acceptable level of maturity (Bumpus, 2013). The NIST has created the Cybersecurity Framework to provide a common language for assuring cybersecurity and help organisations plot their path to a more secure state (Calder, 2018).

The Cybersecurity Framework consists of three parts: the *framework core*, the *implementation tiers*, and the *framework profile* (NIST, 2018).

Table 2 represents the *framework core* which describes a life cycle of five functions that group 20 categories of security controls. These five functions are (1) *identify* (i.e., to identify assets and potential threats), (2) *protect* (i.e., to implement a security baseline), (3) *detect* (i.e., to monitor and control cybersecurity activities that can be considered threats), (4) *respond* (i.e., to respond to a cyber event), and (5) *recover* (i.e., to effectively recover from an incident) (NIST, 2018).

Table 2: NIST Framework core[3]

NIST Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy

[3] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (nist.gov)

	Supply Chain Risk Management
Protect	Identity Management and Access Control
	Awareness and training
	Data Security
	Information protection Processes and Procedures
	Maintenance
	Protective technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recover planning
	Improvements
	Communications

We will use the NIST framework core in our data analysis to map each paper in our sample to the cybersecurity functions and categories.

3. Methodology

SLR studies aim to present a comprehensive evaluation of a research topic (Keele, 2007) by following a structured methodology, i.e., to identify, analyse and interpret information related to that topic (Okoli, 2015). This methodology has proved convenient for studying literature's current state and improvements in a specific domain (B. A. Kitchenham, 2012). In parallel, SLR is an approach for highlighting relevant issues and stressing the urge for further research on the topic (Boell & Cecez-Kecmanovic, 2015). For this purpose, SLRs require understanding the scope of the research by defining a clear objective. This is followed by the identification of various sources of information and defining criteria for selecting the articles (Siddaway, 2014). Translated to this study, Table 3 presents our SLR protocol.

Table 3. Our SLR protocol

The Structure Literature Review (SLR) protocol for this study	
Protocol elements	**Translation to this study**
Research question	Overall RQ: What is the current state of the research on the application of information security and privacy in hospitals? SLR-RQ1: To what extent is the research on the application of information security and privacy in hospitals evolving? SLR-RQ2: Which cybersecurity areas have most frequently been investigated in research on the application of information security and privacy in hospitals? SLR-RQ3: What are the potential research avenues?
Sources of search	Databases: Web of Science, Scopus, AIS Electronic Library, Science Direct, IEEE Xplore Digital Library.
Search terms	Hospital, Cybersecurity, Health, GDPR, Privacy, Information Security.
Search strategy	Peer-reviewed journals and conference papers; theoretical and empirical research; no publication date limit, no topic limit; search terms contained in articles' title, abstract and keywords.
Inclusion criteria	Include only papers containing a combination of search terms, defined in the search queries Include only papers written in English
Exclusion criteria	Exclude unrelated papers, i.e., if they do not explicitly claim addressing the topic of cybersecurity Exclude articles without full access Exclude introduction papers in special issues
Quality criteria	Only peer-reviewed papers are indexed in the databases

Table 3 presents the SLR protocol applied to this research.

To review the application of information security and privacy in hospitals, we analysed the content and metadata of the selected articles. We subdivided our main RQ into three detailed SLR-RQs to collect more knowledge on the subject.

We selected five academic databases (i.e., Web of Science, Scopus, AIS Electronic Library, Science Direct, IEEE Xplore Digital Library) because these databases are recognised for providing access to peer-reviewed publications in an intuitive and structured manner. We decided not to restrict the search to a specific period because the realm of cybersecurity coupled with the healthcare sector is rather new. Therefore, all the results up to May 2021 were considered, which is when our literature search ended.

We searched for articles containing a combination of the following terms in their title, abstract and keywords: “cybersecurity AND health*”; “GDPR AND hospital”; “cybersecurity AND hospital*”; “information security* AND privacy AND health”; “information privacy AND hospital”; and “information security AND privacy AND hospital”. We excluded the duplicates emerging from the search of multiple databases and proceeded to identify the articles’ importance and relevance for our goal. In this stage, we found 302 articles.

We applied the inclusion and exclusion criteria to determine the papers that were relevant to our objective (B. Kitchenham et al., 2009), as shown in Figure 2. In addition to inclusion/exclusion criteria concerning language, setting, sample and publication, we omitted all papers that used the term “hospital” with a different meaning than the one explained in the research background, such as veterinary hospitals.

At the end of this phase, we obtained 62 articles. Based on the full-text reading, the previous criteria were applied again to determine the actual research subject in the selected articles. We thus analysed the remaining papers to verify the relationships between hospitals, cybersecurity and privacy. When we could confirm that an article was linked to at least one domain of cybersecurity, the paper was selected as revealing significance for the objective of this study. We finally selected 58 articles to be included for further analysis (Appendix A).

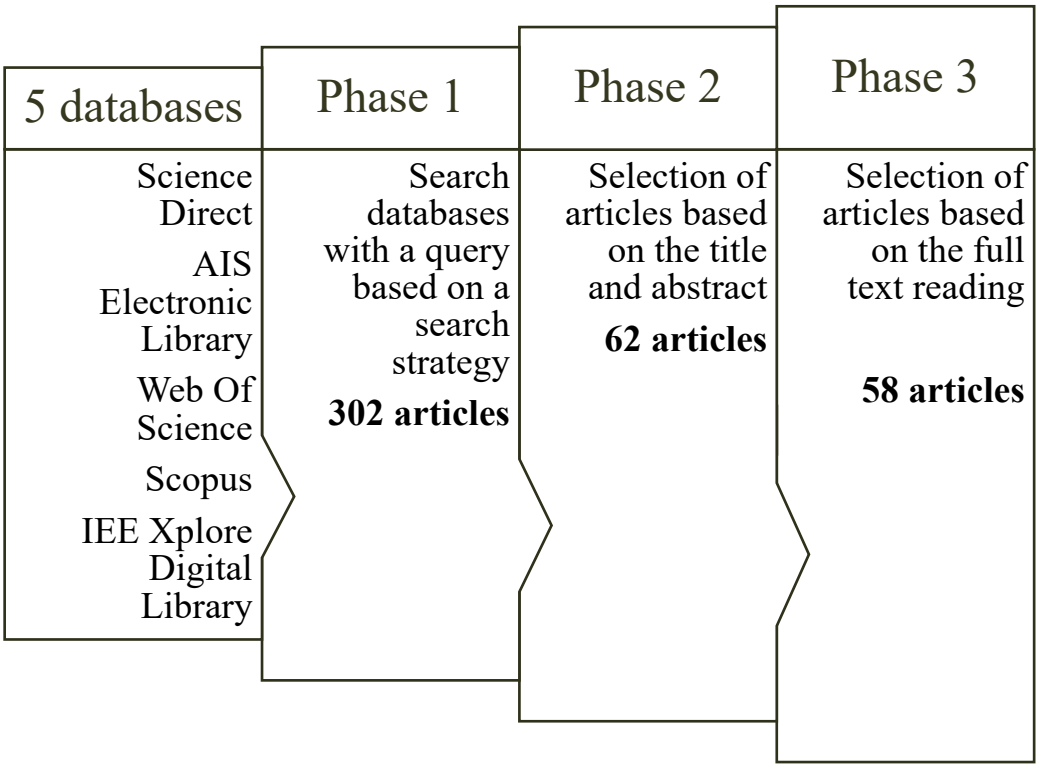

Figure 2: Search and selection of articles considered for this study.

4. Results

A. SLR-RQ1 results

The results for SLR-RQ1 were addressed by classifying the selected articles according to their publication dates (Figure 3) and affiliation of the first authors (Figure 4).

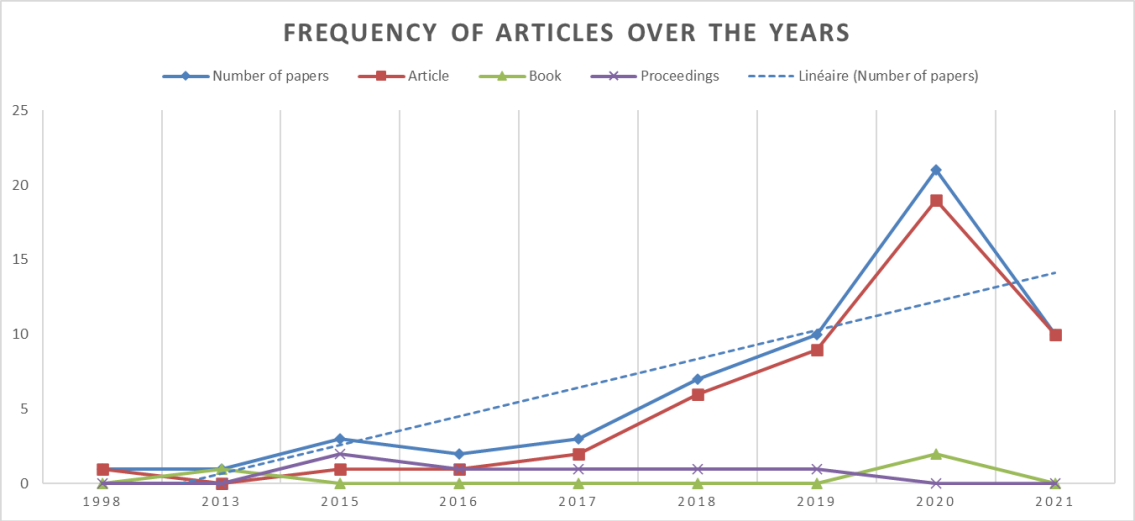

Figure 3: Frequency of articles over the years (N=58)

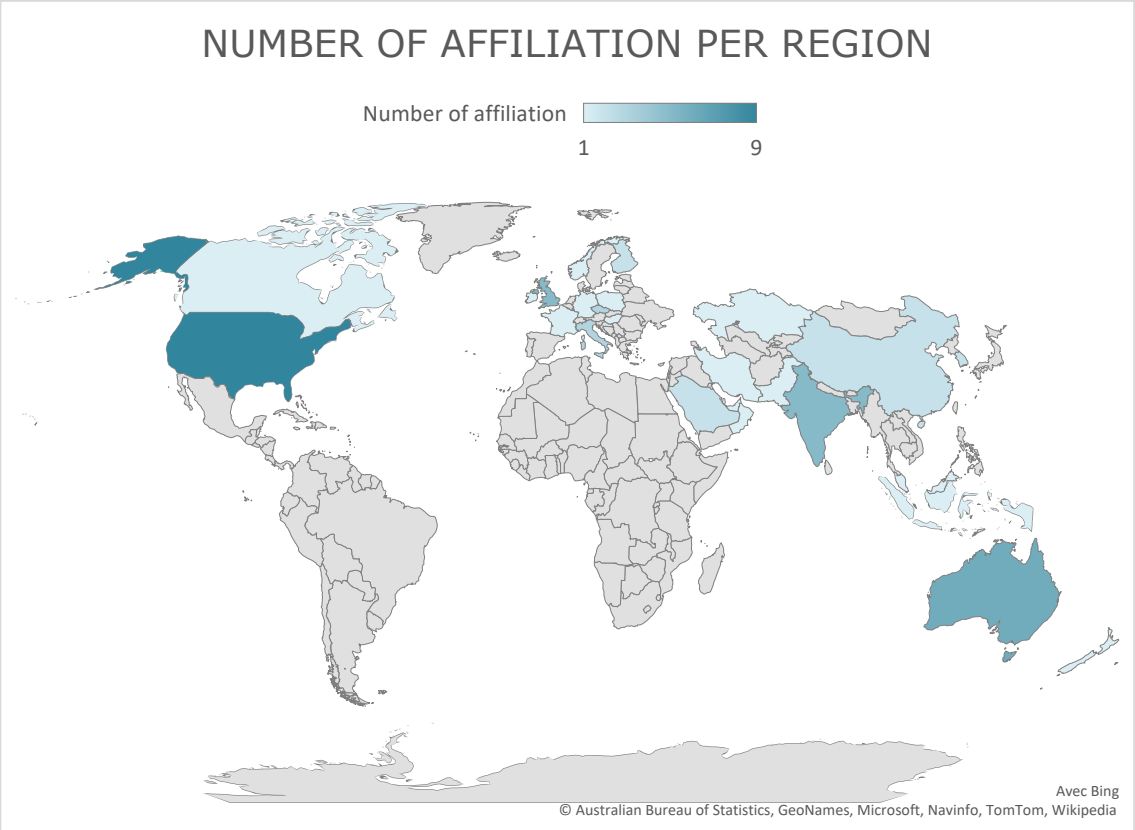

Figure 4: The geographical distribution of the selected papers per country and region, based on first authors' affiliation (N=58)

Figure 3 illustrates that research on cybersecurity in hospitals has increased over the years, especially from 2018 upwards. The countries with five or more papers in our sample are the US (9 papers), Australia (6 papers), India (5 papers) and the UK (5 papers). Furthermore, Figure 4 illustrates that cybersecurity within hospitals is a subject of research worldwide, with papers from various countries. Nonetheless, a possible explanation for the high number of papers from the US, Australia and UK could be the recent attacks targeting hospitals in each of these countries, among others (Muthuppalaniappan & Stevenson, 2021). We identified the first relevant paper of the sample on cybersecurity challenges within hospitals from 1998, and the next contribution was from 2013.

We noticed a significant rise in 2018 (7 papers), 2019 (10 papers), 2020 (21 papers) and 2021 (10 papers). A potential reason for such a rapid evolution could be the implementation of EU policies in 2018, namely, a new regulation in data protection (GDPR) to enhance privacy and cybersecurity across Europe. As matter of fact, we enumerated 14 papers in Europe, excluding the UK, in the period from 2017 to 2021, illustrating the direct impact of GDPR and national privacy regulations.

The COVID-19 pandemic (which started in 2019) could have also brought more focus to the hospitals and could explain the high number of articles related to cybersecurity and privacy within hospitals. We have identified 11 articles referring to COVID-19 in recent papers.

The growing amount of research on this subject might exist also due to the level of technological development in the healthcare sector. We are at the stage of Healthcare

4.0, branded by a focus on medical devices and patient data-monitoring tools (Aceto et al., 2020). We have listed 46 papers addressing such digital innovation.

B. SLR-RQ2 results

For SLR-RQ2, we first matched the selected articles with the ISO 27001 sets of controls. Table 4 shows that clause A.5, related to information security policies, is not covered in our selected articles. This finding is aligned with the controls on compliance (A.18), which are only covered by two articles. Furthermore, Table 4 illustrates that A.11 controls on physical and environmental security are not represented in our sample. A reason for this last observation could be the scope of our literature review, which focuses on information security and privacy rather than physical security. Moreover, Table 4 indicates that the clauses related to human resources (A.7), asset management (A.8) and system configuration (A.14) are discussed in several papers. This could be due to new technologies inserted in hospitals, which demand ever-increasing integration with previous systems, a need for skilled people and continuous interaction with practitioners and patients. In our research sample, 29 papers refer to new technologies.

Table 4: Mapping of ISO 27001 Annex A with our sample. Note: the results are not cumulative, because articles can be classified in more than one set of controls.

Clauses	Name	Number of controls	Number of related sampled articles
A.5	Information Security Policies	2	0

A.6	Organisation of Information Security	7	7
A.7	Human resource Security	6	12
A.8	Asset Management	10	26
A.9	Access Control	14	5
A.10	Cryptography	2	25
A.11	Physical and environmental security	15	0
A.12	Operations security	14	44
A.13	Communication Security	7	0
A.14	System acquisition, development, and maintenance	13	25
A.15	Supplier relationship	5	0
A.16	Information Security Incident management	7	9
A.17	Information Security aspects of business continuity management	4	3
A.18	Compliance	8	2

Next, to further investigate SLR-RQ2, we mapped our selected articles to the five NIST functions by analysing the content of each paper (Table 5). The table shows that "Protect" has collected the most interest. This could be explained by a culture of operational mind set within hospitals (Burns et al., 2015). Many articles (35) matched the

category “information protection, processes and procedures”; 25 explored the category “protective technology”. This could be a consequence of the ever-increasing implementation of new devices (Sari et al., 2020). Articles related to risk assessment received less coverage (three papers). One reason could be the environment in silos of hospitals and the complexity involved in adopting a comprehensive risk assessment methodology (Burns et al., 2015).

Table 5: Mapping of the NIST framework core with our sample. Note: the results are not cumulative, because articles can be classified in more than one set of controls.

NIST Function	Category	Number of related sampled articles
Identify	Asset Management	1
	Business Environment	1
	Governance	2
	Risk Assessment	3
	Risk Management Strategy	1
	Supply Chain Risk Management	0
Protect	Identity Management and Access Control	5
	Awareness and training	14
	Data Security	5
	Information protection Processes and Procedures	35

	Maintenance	0
	Protective technology	25
Detect	Anomalies and Events	9
	Security Continuous Monitoring	6
	Detection Processes	5
Respond	Response planning	0
	Communications	0
	Analysis	2
	Mitigation	2
	Improvements	1
Recover	Recover planning	0
	Improvements	1
	Communications	0

C. SLR-RQ3 results

We set forth on SLR-RQ3 the potential research gaps.

The first open issue for research and practice can be addressing asset identification related to information security and privacy in hospitals. Most of the practices related to security and privacy that were investigated in the papers derive from the technology industry. Contributions in the NIST function “identify” are limited. Two articles tackled the governance section of the “identify” function, and only one paper covered the risk management strategy section of the “identify” function.

A second potential issue for research and practice can be indicated as crisis management and the recovering phase after a security breach. The NIST function "respond" is key to developing tangible methods of restoring critical information such as patient data after a cybersecurity incident. Only 4% of our selected papers covered NIST categories related "respond", while this function will meaningfully impact hospitals' ability to continue treatments when a crisis occurs.

The third perspective for research and practice can be oriented towards exploring the implications of new technologies to "detect" security and privacy risks within hospitals – for instance, delocalising the patient data in the cloud. Only six papers in our set discussed cloud computing within the healthcare sector. However, understanding the privacy and security risks of such evolution can help reduce the risk of patient data breach. Big data and AI in hospitals can be studied from a security and privacy angle to treat patient data more securely. Blockchain technology can also be a topic of interest in providing innovative tools to secure patient data.

Only five papers discussed the impact of people on cybersecurity-related events in hospitals. As humans are the weakest link in cybersecurity, identifying creative ways of continual training and approaches to awareness of the healthcare sector could constitute a fourth possible issue for research and practice.

The fifth subject of research and practice that should be addressed concerns hospitals' organisational structure. In our sample, limited articles covered the implementation of an international framework in privacy and information security specific to hospitals. The HIPAA regulation in the US is intended to define how hospitals can protect themselves against cyber-attacks. However, there is not yet a similar regulation in the EU. Thus, major attention could be given to how to deploy, optimise and manage security and privacy in hospitals.

To continue our investigation of RQ3, Table 6 presents potential topics for future research as identified in the selected articles. Most of the papers identified security and privacy aspects related to IOT as relevant topics for further research.

Table 6: Research agenda
Note: the results are not cumulative, because articles can be classified in more than one set of controls.

Research agenda	Example of topics	Number of papers with this recommendation
1) Big data	How to gather, process and analyse large volumes of personal healthcare data? How to build an efficient data management capability within hospitals? How to ensure anonymisation and encryption of patient data in the context of big data analysis?	16
2) Machine learning	How to optimize the healthcare system and provide intelligent services effectively?	23

	How to integrate machine learning and blockchain in the context of healthcare systems? What are the risks of AI and machine learning methods in hospitals?	
3) Internet of Things (IOT)	What are the privacy issues related to medical devices (geolocation, monitoring, information sharing)? What are the security issues of medical devices' sensors and how to mitigate these risks? How IOT and 5G are related in the context of smart healthcare?	45
4) Cloud Computing	What are the risks and advantages of Cloud computing for patient data?	27
5) Blockchain	How blockchain can be used to enhance security and privacy risks of medical devices? How to improve blockchain stability for reliability purposes in the context of the healthcare?	32

6) Standards and regulations	How to vet new technologies related to medical devices from a security and privacy perspective? How to define a roadmap of an independent and trustworthy third party competent to audit hospitals' security and privacy compliance?	10

5. Discussion

Our study confirms that the attack surface of hospitals is large and has even expanded due to the introduction of new Internet-based technologies (Ahmed et al., 2019). The sharp rise of the IOT in the healthcare sector plays a significant role in applying a recognizable digital innovation to capture large amounts of patient data (Aceto et al., 2020). By adopting cloud computing, blockchain and big data tools, hospitals have an opportunity to change their cybersecurity posture. At the same time, this has introduced new risks in their environments (Huang et al., 2018). Therefore, it might be worth looking at new architecture models that can ensure integration of existing technologies and advanced methods (Stergiou et al., 2022).

Compared to previous reviews on information security and privacy in hospitals, our study focused on discovering research gaps considering the domains covered by two widely known cybersecurity frameworks: ISO/IEC 27001 and NIST. The most important findings worth considering for researchers and practitioners are:

- A lack of research on sectorial regulations in cybersecurity and privacy within hospitals. This could be linked to the limited number of articles (10) related to standards and regulations in our research agenda.
- The necessity of more research on secure large-scale efficient data management (Plageras et al., 2017) which could impact hospitals regarding their approach to cybersecurity.
- The culture within hospitals can influence the implementation of security and privacy measures (Said et al., 2014).

We learned from our literature review that ineffective measures to prevent hospitals from information security attacks and privacy issues may lead to security breaches in which hackers can gain full access to patient email accounts, messages and reports (Shi et al., 2020). Blockchain is a growing technology that comes with several viable sharing and storing characteristics, including decentralisation, immutability, transparency and traceability (Abu-elezz et al., 2020). The limitations of blockchain technology utilisation within the healthcare field include scalability issues, interoperability and lack of technical expertise, which could be the reason many healthcare organisations remain hesitant to use it (Hathaliya & Tanwar, 2020).

However, security and privacy risks should not stop hospitals from exploring digital innovation brought about by technological opportunities (Stergiou et al., 2021), particularly new IoT-based medical devices (S. Anderson & Williams, 2018). Twenty-five papers in our set emphasized this concern. Further, we noticed that mobile health (mHealth) is a growing field that enables individuals to monitor their health status and facilitates the sharing of medical records (Zubaydi et al., 2015). Patient data become more accessible through safeguarding mobile agents that are transmitted from one location to the other (Keshta & Odeh, 2020). However, application developers are not transparent

about data protection and introduce risks related to privacy-by-default principles (Sunyaev et al., 2014). For instance, research on highly used mHealth applications in four developed countries found that the majority of the included applications for analysis shared personal data with third parties (Grundy et al., 2019).

6. Conclusion

This article identified research gaps and opportunities regarding information security and privacy in hospitals. Our findings are based on a systematic review of the research following a rigorous SLR protocol. We used two cybersecurity frameworks to analyse the papers found to be relevant (58 papers in total): the NIST framework and the ISO 27001 standard. Positioning the subjects addressed by the papers in these frameworks allowed us to uncover areas well or less investigated. As these frameworks provide a holistic picture of points of attention and activities related to the implementation of cybersecurity, the areas having received no or little research attention are worth focusing on in future research.

More specifically, the review result showed that the technical areas of cybersecurity were most tackled in the sample, and less attention was paid to other realms such as management, policies, processes, and culture. If the literature on cybersecurity in hospitals is increasing, it is still relatively limited compared to the level of threat facing patient data.

Thus, our main contribution is providing a research agenda by identifying key domains in information security and privacy where further research in hospitals is needed.

Last, we urge security and privacy practitioners in hospitals to ensure continuous awareness to bring about cultural change. Also, we call for more research in integration of advanced methods concerning novel architectures to ensure a comprehensive approach in handling information security and privacy in hospitals. Our own future research will

be the security and privacy aspects related to the use of IoT in hospitals, with a focus on how to apply Privacy by Design methodologies to IoT-based medical devices.

Author Contributions

Conceptualization, S.A. and A.V.L.; methodology, A.V.L. and S.A.; writing—original draft preparation, S.A.; writing—review and editing, A.V.L. and G.P.; supervision, A.V.L. and G.P. The authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

The underlying data for the Systematic Literature Review are available at the following location: https://data.mendeley.com/datasets/w69674f3hy/draft?a=3b61f725-8414-4ee5-be87-8fcfce45a830

Conflicts of Interest

The authors declare no conflict of interest.

Appendix A. Literature sample (N = 58)

P01	Abu-elezz, I., Hassan, A., Nazeemudeen, A., Househ, M., & Abd-alrazaq, A. (2020). The benefits and threats of blockchain technology in healthcare: A scoping review. International Journal of Medical Informatics, 142, 104246. https://doi.org/10.1016/j.ijmedinf.2020.104246
P02	Aceto, G., Persico, V., & Pescapé, A. (2020). Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0. Journal of Industrial Information Integration, 18, 100129. https://doi.org/10.1016/j.jii.2020.100129
P03	Ahmed, Y., Naqvi, S., & Josephs, M. (2019). Cybersecurity Metrics for Enhanced Protection of Healthcare IT Systems. 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), 2019-May, 1–9. https://doi.org/10.1109/ISMICT.2019.8744003
P04	Alexander, G. L., Georgiou, A., Doughty, K., Hornblow, A., Livingstone, A., Dougherty, M., Jacobs, S., & Fisk, M. J. (2020). Advancing health information technology roadmaps in long term care. International Journal of Medical Informatics, 136, 104088. https://doi.org/10.1016/j.ijmedinf.2020.104088
P05	Alraja, M. N., Farooque, M. M. J., & Khashab, B. (2019). The Effect of Security, Privacy, Familiarity, and Trust on Users' Attitudes Toward the Use of the IoT-Based Healthcare: The Mediation Role of Risk Perception. IEEE Access, 7, 111341–111354. https://doi.org/10.1109/ACCESS.2019.2904006
P06	Anderson, S., & Williams, T. (2018). Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge? Computer Standards & Interfaces, 56, 134–143. https://doi.org/10.1016/j.csi.2017.10.001
P07	Athinaiou, M., Mouratidis, H., Fotis, T., & Pavlidis, M. (2020). A Conceptual Redesign of a Modelling Language for Cyber Resiliency of Healthcare Systems. Katsikas S. (Ed.), Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 11980 LNCS (pp. 140–158). Springer. https://doi.org/10.1007/978-3-030-42048-2_10

P08	Attaran, M. (2020). Blockchain technology in healthcare: Challenges and opportunities. International Journal of Healthcare Management, 1–14. https://doi.org/10.1080/20479700.2020.1843887
P09	Barad, M. (2019). Linking Cyber Security Improvement Actions in Healthcare Systems to Their Strategic Improvement Needs. Procedia Manufacturing, 39, 279–286. https://doi.org/10.1016/j.promfg.2020.01.335
P10	Bellekens, X., Hamilton, A., Seeam, P., Nieradzinska, K., Franssen, Q., & Seeam, A. (2016). Pervasive eHealth services a security and privacy risk awareness survey. 2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA), 1–4. https://doi.org/10.1109/CyberSA.2016.7503293
P11	Chacko, A., & Hayajneh, T. (2018). Security and Privacy Issues with IoT in Healthcare. EAI Endorsed Transactions on Pervasive Health and Technology, 0(0), 155079. https://doi.org/10.4108/eai.13-7-2018.155079
P12	Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing. IEEE Access, 7, 74361–74382. https://doi.org/10.1109/ACCESS.2019.2919982
P13	Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. PLOS ONE, 15(12), e0243043. https://doi.org/10.1371/journal.pone.0243043
P14	Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. Computer Science Review, 40, 100361. https://doi.org/10.1016/j.cosrev.2021.100361

P15	Crozier-Shaw, G., Hughes, A. J., Cashman, J., & Synnott, K. (2021). Instant messaging apps and data protection: combining to improve hip fracture care? Irish Journal of Medical Science (1971 -). https://doi.org/10.1007/s11845-021-02612-4
P16	Felkai, P., & Lengyel, I. (2019). Kéretlen e-mailek az orvos postafiókjában: ezek veszélyei az egészségnevelésre, a betegtájékoztatásra és a tudományos munkára. Orvosi Hetilap, 160(43), 1706–1710. https://doi.org/10.1556/650.2019.31531
P17	Finocchiaro, G. (2018). Protection of privacy and cyber risk in healthcare. Pharmaceuticals Policy and Law, 19(3–4), 121–123. https://doi.org/10.3233/PPL-180462
P18	Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., & Baker, T. (2018). Security threats to critical infrastructure: the human factor. The Journal of Supercomputing, 74(10), 4986–5002. https://doi.org/10.1007/s11227-018-2337-2
P19	Habib, M. A., Faisal, C. M. N., Sarwar, S., Latif, M. A., Aadil, F., Ahmad, M., Ashraf, R., & Maqsood, M. (2019). Privacy-based medical data protection against internal security threats in heterogeneous Internet of Medical Things. International Journal of Distributed Sensor Networks, 15(9), 155014771987565. https://doi.org/10.1177/1550147719875653
P20	Hajder, M., Kolbusz, J., Hajder, P., Nycz, M., & Liput, M. (2020). Data Security Platform Model in Networked Medical IT Systems based on Statistical Classifiers and ANN. Procedia Computer Science, 176, 3682–3691. https://doi.org/10.1016/j.procs.2020.09.018
P21	Hassija, V., Chamola, V., Bajpai, B. C., Naren, & Zeadally, S. (2021). Security issues in implantable medical devices: Fact or fiction? Sustainable Cities and Society, 66, 102552. https://doi.org/10.1016/j.scs.2020.102552

P22	Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. Computer Communications, 153, 311–335. https://doi.org/10.1016/j.comcom.2020.02.018
P23	Husák, M., Neshenko, N., Pour, M. S., Bou-Harb, E., & Čeleda, P. (2018). Assessing Internet-wide Cyber Situational Awareness of Critical Sectors. Proceedings of the 13th International Conference on Availability, Reliability and Security, 1–6. https://doi.org/10.1145/3230833.3230837
P24	Ihanus, J., & Kokkonen, T. (2020). Modelling Medical Devices with Honeypots. In B. S. K. Y.
P25	Galinina O. Andreev S. (Ed.), Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 12525 LNCS (pp. 295–306). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-030-65726-0_26
P26	Ioane, J., Knibbs, C., & Tudor, K. (2021). The challenge of security and accessibility: Critical perspectives on the rapid move to online therapies in the age of COVID-19. Psychotherapy and Politics International, 19(1). https://doi.org/10.1002/ppi.1581
P27	Kaplan, B. (2020). REVISITING HEALTH INFORMATION TECHNOLOGY ETHICAL, LEGAL, and SOCIAL ISSUES and EVALUATION: TELEHEALTH/TELEMEDICINE and COVID-19. International Journal of Medical Informatics, 143, 104239. https://doi.org/10.1016/j.ijmedinf.2020.104239
P28	Keshta, I., & Odeh, A. (2020). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal. https://doi.org/10.1016/j.eij.2020.07.003
P29	Kim, H., Kim, S.-W., Park, E., Kim, J. H., & Chang, H. (2020). The role of fifth-generation mobile technology in prehospital emergency care: An opportunity to support paramedics. Health Policy and Technology, 9(1), 109–114. https://doi.org/10.1016/j.hlpt.2020.01.002

P30	Kim, Y.-W., Cho, N., & Jang, H.-J. (2018). Trends in Research on the Security of Medical Information in Korea: Focused on Information Privacy Security in Hospitals. Healthcare Informatics Research, 24(1), 61. https://doi.org/10.4258/hir.2018.24.1.61
P31	Kintzlinger, M., & Nissim, N. (2019). Keep an eye on your personal belongings! The security of personal medical devices and their ecosystems. Journal of Biomedical Informatics, 95, 103233. https://doi.org/10.1016/j.jbi.2019.103233
P32	Kolanska, K., Chabbert-Buffet, N., Daraï, E., & Antoine, J.-M. (2021). Artificial intelligence in medicine: A matter of joy or concern? Journal of Gynecology Obstetrics and Human Reproduction, 50(1), 101962. https://doi.org/10.1016/j.jogoh.2020.101962
P33	Langer, S. G. (2017). Cyber-Security Issues in Healthcare Information Technology. Journal of Digital Imaging, 30(1), 117–125. https://doi.org/10.1007/s10278-016-9913-x
P34	Martin, G., Kinross, J., & Hankin, C. (2017). Effective cybersecurity is fundamental to patient safety. BMJ, 357, j2375. https://doi.org/10.1136/bmj.j2375
P35	Marvel, L. M., Brown, S., Neamtiu, I., Harang, R., Harman, D., & Henz, B. (2015). A framework to evaluate cyber agility. MILCOM 2015 - 2015 IEEE Military Communications Conference, 2015-Decem, 31–36. https://doi.org/10.1109/MILCOM.2015.7357414
P36	Mulligan, E. (1998). Protecting patient confidentiality in hospitals. Australian Health Review, 21(3), 67. https://doi.org/10.1071/AH980067
P37	Muthuppalaniappan, M., & Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. International Journal for Quality in Health Care, 33(1). https://doi.org/10.1093/intqhc/mzaa117

P38	Nair, M. M., Tyagi, A. K., & Goyal, R. (2019). Medical Cyber Physical Systems and Its Issues. Procedia Computer Science, 165, 647–655. https://doi.org/10.1016/j.procs.2020.01.059
P39	Owens, B. (2020). How hospitals can protect themselves from cyber attack. Canadian Medical Association Journal, 192(4), E101–E102. https://doi.org/10.1503/cmaj.1095841
P40	Palanisamy, R., Norman, A. A., & Kiah, M. L. M. (2020). Compliance with bring your own device security policies in organizations: A systematic literature review. Computers & Security, 98, 101998. https://doi.org/10.1016/j.cose.2020.101998
P41	Pavlík, L., Chytilová, E., & Zimmermannová, J. (2021). Security Aspects of Healthcare Organization from the Perspective of Digitization of Facility Management. WSEAS TRANSACTIONS ON BUSINESS AND ECONOMICS, 18, 360–366. https://doi.org/10.37394/23207.2021.18.36
P42	Pool, J., Akhlaghpour, S., & Fatehi, F. (2020). Towards a contextual theory of Mobile Health Data Protection (MHDP): A realist perspective. International Journal of Medical Informatics, 141, 104229. https://doi.org/10.1016/j.ijmedinf.2020.104229
P43	Rajamäki, J., & Pirinen, R. (2017). Towards the cyber security paradigm of ehealth: Resilience and design aspects. In N. K. (Ed.), AIP Conference Proceedings (Vol. 1836, p. 020029). American Institute of Physics Inc. https://doi.org/10.1063/1.4981969
P44	Ramadan, R. A., Aboshosha, B. W., Alshudukhi, J. S., Alzahrani, A. J., El-Sayed, A., & Dessouky, M. M. (2021). Cybersecurity and Countermeasures at the Time of Pandemic. Journal of Advanced Transportation, 2021, 1–19. https://doi.org/10.1155/2021/6627264
P45	Razaque, A., Amsaad, F., Jaro Khan, M., Hariri, S., Chen, S., Siting, C., & Ji, X. (2019). Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical

Domain. IEEE Access, 7, 168774–168797. https://doi.org/10.1109/ACCESS.2019.2950849

P46	Reshmi, T. R. (2021). Information security breaches due to ransomware attacks - a systematic literature review. International Journal of Information Management Data Insights, 1(2), 100013. https://doi.org/10.1016/j.jjimei.2021.100013
P47	Sajedi, H., & Rahbar Yaghobi, S. (2020). Information hiding methods for E-Healthcare. Smart Health, 15, 100104. https://doi.org/10.1016/j.smhl.2019.100104
P48	Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber Risk in Health Facilities: A Systematic Literature Review. Sustainability, 12(17), 7002. https://doi.org/10.3390/su12177002
P49	Sari, P. K., Handayani, P. W., & Hidayanto, A. N. (2020). Security Value Issues on eHealth Implementation in Indonesia. IOP Conference Series: Materials Science and Engineering, 879(1), 012040. https://doi.org/10.1088/1757-899X/879/1/012040
P50	Seifert, D., & Reza, H. (2016). A Security Analysis of Cyber-Physical Systems Architecture for Healthcare. Computers, 5(4), 27. https://doi.org/10.3390/computers5040027
P51	Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Computers & Security, 97, 101966. https://doi.org/10.1016/j.cose.2020.101966
P52	Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. Journal of Network and Computer Applications, 160, 102642. https://doi.org/10.1016/j.jnca.2020.102642

P53	Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. Computers in Biology and Medicine, 129, 104130. https://doi.org/10.1016/j.compbiomed.2020.104130
P54	Tomar, R. (2019). Analysis Against DDOS Flooding Attacks in Healthcare System using Artificial Neural Network. International Journal of Advanced Trends in Computer Science and Engineering, 8(1.5), 405–410. https://doi.org/10.30534/ijatcse/2019/6481.52019
P55	Tse, Z. T. H., Xu, S., Fung, I. C.-H., & Wood, B. J. (2015). Cyber-attack risk low for medical devices. Science, 347(6228), 1323–1324. https://doi.org/10.1126/science.347.6228.1323-b
P56	Venkatasubramanian, K. K., Nabar, S., Gupta, S. K. S., & Poovendran, R. (2013). Cyber Physical Security Solutions for Pervasive Health Monitoring Systems. In User-Driven Healthcare (Vol. 1, pp. 447–465). IGI Global. https://doi.org/10.4018/978-1-4666-2770-3.ch022
P57	Walker-Roberts, S., Hammoudeh, M., & Dehghantanha, A. (2018). A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. IEEE Access, 6, 25167–25177. https://doi.org/10.1109/ACCESS.2018.2817560
P58	Wurmb, T., Kippnich, M., Schwarzmann, G., Mehlhase, J., Valotis, A., Firnkes, T., Braungardt, J., & Ertl, G. (2020). Vollausfall der Informationstechnologie im Krankenhaus. Der Unfallchirurg, 123(6), 443–452. https://doi.org/10.1007/s00113-020-00797-4

References

A. Sunyaev, T. Dehling, P.L. Taylor, K. D. M., Policies, A. and quality of mobile health app privacy, & J. Am. Med. Inform. Assoc., 22 (2014), pp. e28-e33. (2014).

Policies, Availability and quality of mobile health app privacy. *J. Am. Med. Inform.*

Aarestrup, F. M., Albeyatti, A., Armitage, W. J., Auffray, C., Augello, L., Balling, R., Benhabiles, N., Bertolini, G., Bjaalie, J. G., Black, M., Van Den Bulcke, M., & Van Oyen, H. (2020). Towards a European health research and innovation cloud (HRIC). *Genome Medicine*, *12*(1). https://doi.org/10.1186/s13073-020-0713-z

Abu-elezz, I., Hassan, A., Nazeemudeen, A., Househ, M., & Abd-alrazaq, A. (2020). The benefits and threats of blockchain technology in healthcare: A scoping review. *International Journal of Medical Informatics*, *142*, 104246. https://doi.org/10.1016/j.ijmedinf.2020.104246

Aceto, G., Persico, V., & Pescapé, A. (2020). Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0. *Journal of Industrial Information Integration*, *18*, 100129. https://doi.org/10.1016/j.jii.2020.100129

Ahmed, Y., Naqvi, S., & Josephs, M. (2019). Cybersecurity Metrics for Enhanced Protection of Healthcare IT Systems. *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, *2019-May*, 1–9. https://doi.org/10.1109/ISMICT.2019.8744003

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers and Security*. https://doi.org/10.1016/S0167-4048(03)00407-3

Anderson, S., & Williams, T. (2018). Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge? *Computer Standards & Interfaces*, *56*, 134–143. https://doi.org/10.1016/j.csi.2017.10.001

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise Management*, *6*(4), 279. https://doi.org/10.1504/IJIEM.2010.035624

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J. M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*(1), 1–10. https://doi.org/10.1186/s12911-020-01161-7

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. In *MIS Quarterly: Management Information Systems*. https://doi.org/10.2307/41409971

Boell, S. K., & Cecez-Kecmanovic, D. (2015). On being "systematic" in literature reviews in IS. In *Journal of Information Technology*. https://doi.org/10.1057/jit.2014.26

Brenner, J. (2007). ISO 27001: Risk management and compliance. *Risk Management*.

Bumpus, W. (2013). NIST Cloud Computing Standards Roadmap. *NIST Cloud Computing Standards*.

Burns, A. J., Johnson, M. E., & Honeyman, P. (2016). A Brief Chronology of Medical Device Security. *COMMUNICATIONS OF THE ACM*, *59*(10), 66–72. https://doi.org/10.1145/2890488

Burns, A. J., Young, J., Roberts, T., Courtney, J., & Ellis, T. S. (2015). Exploring the Role of Contextual Integrity in Electronic Medical Record (EMR) System Workaround Decisions: An Information Security and Privacy Perspective. *AIS Transactions on Human-Computer Interaction*, *7*(3), 142–165. https://doi.org/10.17705/1thci.00070

Calder, A. (2018). NIST Cybersecurity Framework. In *NIST Cybersecurity Framework*. IT Governance Publishing. https://doi.org/10.2307/j.ctv4cbhfx

Correia, L. S., Correia, R. C., & Rodrigues, P. P. (2019). Illegitimate HIS access by

healthcare professionals: scenarios, use cases and audit trail-based detection model. *Procedia Computer Science*, *164*, 629–636. https://doi.org/https://doi.org/10.1016/j.procs.2019.12.229

Crutzen, R., Ygram Peters, G.-J., & Mondschein, C. (2019). Why and how we should care about the General Data Protection Regulation. *Psychology and Health*, *34*(11), 1347–1357. https://doi.org/10.1080/08870446.2019.1606222

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295–316. https://doi.org/10.1057/ejis.2012.23

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *04*(02), 92–100. https://doi.org/10.4236/jis.2013.42011

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, *46*(3), 541–562. https://doi.org/10.1016/j.jbi.2012.12.003

Finch, J. (1994). Hospitals: definition and classification. In *Speller's Law Relating to Hospitals* (pp. 1–17). Springer US. https://doi.org/10.1007/978-1-4899-7122-7_1

Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatika*, *58*(3), 273–286. https://doi.org/10.1080/00051144.2017.1407022

Guiora, A. N. (2017). What is cybersecurity? In *Cybersecurity* (pp. 15–34). Routledge. https://doi.org/10.1201/9781315370231-2

Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computer Communications*, *153*, 311–335.

https://doi.org/10.1016/j.comcom.2020.02.018

ISO. (2013). ISO/IEC 27001:2013. *Information Technology — Security Techniques — Information Security Management Systems — Requirements*.

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research*, *20*(5), e10059. https://doi.org/10.2196/10059

Keele, S. (2007). Guidelines for performing systematic literature reviews in software engineering. In *Technical report, Ver. 2.3 EBSE Technical Report. EBSE*.

Keshta, I., & Odeh, A. (2020). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*. https://doi.org/10.1016/j.eij.2020.07.003

Kitchenham, B. A. (2012). Systematic review in software engineering. *Proceedings of the 2nd International Workshop on Evidential Assessment of Software Technologies - EAST '12*, 1. https://doi.org/10.1145/2372233.2372235

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering - A systematic literature review. In *Information and Software Technology*. https://doi.org/10.1016/j.infsof.2008.09.009

Kosseff, J. (2018). Defining cybersecurity law. In *Iowa Law Review*.

Masrom, M., & Rahimly, A. (2015). Overview of Data Security Issues in Hospital Information Systems. *Pacific Asia Journal of the Association for Information Systems*, *7*(4), 51–66. https://doi.org/10.17705/1pais.07404

Muthuppalaniappan, M., & Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal for Quality in Health Care*, *33*(1). https://doi.org/10.1093/intqhc/mzaa117

Naconha, A. E. (2021). *A Cybersecurity Model for the Health Sector: A Case Study of Hospitals in Nairobi, Kenya*. *4*(1), 6. http://erepo.usiu.ac.ke/11732/6742

NIST. (2013). NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. *NIST SP-800-53 Ar4*. https://doi.org/10.6028/NIST.SP.800-53Ar4

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity [v1.1 Draft]. *National Institute of Standards and Technology*.

Okoli, C. (2015). A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems*. https://doi.org/10.17705/1cais.03743

Plageras, A. P., Stergiou, C., Kokkonis, G., Psannis, K. E., Ishibashi, Y., Kim, B.-G., & Gupta, B. B. (2017). Efficient Large-scale Medical Data (eHealth Big Data) Analytics in Internet of Things. *2017 IEEE 19th Conference on Business Informatics (CBI)*, *2*, 21–27. https://doi.org/10.1109/CBI.2017.3

Q. Grundy, K. Chiu, F. Held, A. Continella, L. Bero, R. H. (2019). Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. *BMJ*.

Said, A. R., Abdullah, H., Uli, J., & Mohamed, Z. A. (2014). Relationship between Organizational Characteristics and Information Security Knowledge Management Implementation. *Procedia - Social and Behavioral Sciences*, *123*, 433–443. https://doi.org/https://doi.org/10.1016/j.sbspro.2014.01.1442

Sari, P. K., Handayani, P. W., & Hidayanto, A. N. (2020). Security Value Issues on eHealth Implementation in Indonesia. *IOP Conference Series: Materials Science and Engineering*, *879*(1), 012040. https://doi.org/10.1088/1757-899X/879/1/012040

Shabani, M., & Borry, P. (2018). Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. *EUROPEAN JOURNAL OF HUMAN GENETICS*, *26*(2), 149–156. https://doi.org/10.1038/s41431-017-0045-7

Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & Security*, *97*, 101966. https://doi.org/10.1016/j.cose.2020.101966

Siddaway, A. (2014). What is a systematic literature review and how do I do one? *University of Stirling*.

Sipior, J. C., & Ward, B. T. (2001). Cyberliability: Is the Chief Privacy Officer the Solution? *Ecis*, 177-187 ST-Cyberliability: Is the Chief Privacy. 20010103.pdf

Stergiou, C. L., Psannis, K. E., & Gupta, B. B. (2021). IoT-Based Big Data Secure Management in the Fog Over a 6G Wireless Network. *IEEE Internet of Things Journal*, *8*(7), 5164–5171. https://doi.org/10.1109/JIOT.2020.3033131

Stergiou, C. L., Psannis, K. E., & Gupta, B. B. (2022). InFeMo: Flexible Big Data Management Through a Federated Cloud System. *ACM Transactions on Internet Technology*, *22*(2), 1–22. https://doi.org/10.1145/3426972

Zubaydi, F., Saleh, A., Aloul, F., & Sagahyroon, A. (2015). Security of mobile health (mHealth) systems. *2015 IEEE 15th International Conference on Bioinformatics and Bioengineering (BIBE)*, 1–5. https://doi.org/10.1109/BIBE.2015.7367689