Exploring Current Challenges on Security and Privacy in an Operational eHealth Information System

Article *in* Advances in Science Technology and Engineering Systems Journal · April 2024

DOI: 10.25046/aj090206

5 authors, including:

Viktor Denkovski
University American College Skopje
19 PUBLICATIONS **16** CITATIONS
SEE PROFILE

Irena Stojmenovska
University American College Skopje
33 PUBLICATIONS **36** CITATIONS
SEE PROFILE

Goce Gavrilov
University American College Skopje
26 PUBLICATIONS **125** CITATIONS
SEE PROFILE

Vladimir Radevski
South East European University
23 PUBLICATIONS **131** CITATIONS
SEE PROFILE

ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 9, No. 2, 45-54 (2024)

www.astesj.com

Special Issue on Computing, Engineering and Multidisciplinary Sciences

ASTESJ

ISSN: 2415-6698

Exploring Current Challenges on Security and Privacy in an Operational eHealth Information System

Viktor Denkovski[*, 1], Irena Stojmenovska[1], Goce Gavrilov[1], Vladimir Radevski[1], Vladimir Trajkovik[2]

[1]*University American College Skopje, School of Computer Science and Information Technology, Skopje, 1000, North Macedonia*

[2]*University "Ss. Cyril and Methodius", Faculty of Computer Science and Engineering, Skopje, 1000, North Macedonia*

ARTICLE INFO

Article history:
Received:27 February, 2024
Revised: 08 March, 2024
Accepted: 05 April, 2024
Online: 16 April, 2024

Keywords:
eHealth Information System
Security and Privacy Issues
Medical Providers
eHealth Challenges

ABSTRACT

Bearing in mind that patient data is extremely sensitive, it is crucial to establish strong protection when the security and privacy of healthcare data are concerned. Prioritizing data security and privacy is essential for the overall healthcare industry in order to maintain the reliability of electronic healthcare (eHealth) information systems. This study explores the gathered data and information from the surveys and interviews by looking at the security and privacy concerns in using eHealth information technologies. The surveys and interviews were performed on the medical practitioners in N. Macedonia. The main goal is to find out how well-informed are the medical practitioners on the already in-place privacy measures that have been implemented by the medical authorities and to assess their attitudes regarding the need for additional improvements of the system. From the executed interviews, eight healthcare professionals participated in a thorough email interview in order to discover security and privacy issues associated with eHealth systems usage. This information served as the groundwork for administrating an online survey, to which 370 medical practitioners responded from primary and secondary healthcare. The findings emphasize how essential it is to promptly address the system usability concerns on the security and privacy procedures that are implemented when using eHealth technologies.

1. Introduction

This paper is an extension of work originally presented at the 2023 IEEE International Mediterranean Conference on Communications and Networking (MeditCom) [1] to highlight how critical it is to promptly tackle system usability issues related to privacy and security protocols while utilizing eHealth technologies. In recent years there have been revolutionary developments concerning the integration of eHealth information technology, changing the delivery of healthcare services, and providing several benefits, such as raised efficiency and improved accessibility to medical data [2, 3]. Technology has shown increased development that has sped up the integration of eHealth systems way above initial expectations. In 2004, the European Union (EU) established the eHealth systems as a national strategy and policy after realizing their crucial role play in today's modernized healthcare [4]. The research and development strategies from the EU are actively supporting the international progress of the eHealth systems promoting non-EU and EU country cooperation [4].

Even before progressing to national projects, the deployment of eHealth systems needs to go under extensive research and testing in order to address the adaptation and ethical concerns [5]. The mere fact that N. Macedonia's eHealth system was initially implemented without following any clear national policies or strategies indicates the need for additional financial support and support from the government to ensure a smooth national integration later on [6, 7].

The main purposes of electronic health systems are making the medical staff's paperwork easier, lowering costs, and raising satisfaction [8]. To enhance the quality of health care services, well-defined workflow procedures and online data exchange between primary and secondary care facilities must be implemented and adopted [9]. Furthermore, using eHealth technologies makes it much simpler to contact medical specialists, especially those who are working in big cities and larger hospitals. This promotes cooperation in overall health care and improves patient accessibility [8].

To increase efficiency in managing patients and saving paperwork, eHealth systems are an essential tool for patient management and data sharing. This involves digitizing,

[*]Corresponding Author: Viktor Denkovski, viktor.denkovski@uacs.edu.mk

https://dx.doi.org/10.25046/aj090206

exchanging, and archiving all relevant information [7]. However, worries over the security and privacy of the patient's private medical information are raised by the growing dependencies on digital platforms. Trust maintenance in the health care systems and also guaranteeing the patient's data privacy and security requires safeguarding the patient data from illegal breaches, access, and misuse [10]. In alignment with the regulatory protocols, people must be guaranteed that their data is being secured and that the security of digital data is being considered a top priority in eHealth systems [7].

Per a systematic study in [11], the usage of big data analysis and its applications in the healthcare industry has emerged recently in several studies and research projects. Three modules comprise the health care system's structure, of which, medical practitioners, medical consumers, and health services related to medical treatment, like research and health insurance. Furthermore, although it is still in its early stages, the pharmacy business and shareholders started their analysis of big data even more regularly in order to gain knowledge and an overview of numerous activities related to their sector [12].

By the end of 2021, 22 nations that were already a part of the digital service infrastructure for eHealth systems, began exchanging patient information and electronic prescriptions, indicating that healthcare data digitalization in some EU countries was already at an advanced stadium [13]. According to the World Health Organization (WHO) Regional Office for Europe in [14], research of healthcare big data in the healthcare sector presented vital importance, however, they were not sufficiently explored, and there were only a few methods and arrangements that offered help in this field. Having in mind this assessment, just 13% (six nations) of the EU had integrated national policies and rules in motion for big data in this area, while the private sector controlled just a small portion of this, or just 9% (four nations). The commercial sector would take over and seize the chance to capitalize on the potential of big data analysis in the healthcare industry if the public medical authorities fail to investigate this issue.

As was already pointed out above, big data in healthcare information systems presents several security and privacy issues when it comes to patient medical records. At the top, data centers that house sensitive data possess various levels of security. Because of this, it was unable to directly apply conventional security options and solutions to sizable and diverse data sets [15]. The complexity of security in many software systems that can handle different sources and data formats is compounded by the growing demand for cloud solutions in the healthcare sector [16]. Big data had to be properly maintained for this reason to be made available for data analysis.

Utilizing the accumulated big data for any kind of progress across all industries may present various difficulties. The lifecycle of the data was divided into data, management, and process classification when it comes to those difficulties [17]. The representation of data characteristics (variety, visualization, volume, variability, etc.) was one type of such difficulty. Security and privacy issues presented one of the challenges to be managed, also, issues that arise during data processing (analysis and modeling, data mining and implementation, etc.), and the absence of understanding the data. According to [18], management of big data must be improved by using operations of cleaning, processing, analyzing, securing, and granting access to the data due to its lack of flexibility, scalability, and performance. Furthermore, security and privacy protection were essential for the widespread usage of big data in all areas especially in the healthcare sector. Thus, the privacy and security issues related to the topic at hand were breakdown into categories that address infrastructure security (cloud security DoS attacks, Hadoop), data management (auditing and monitoring, key management, and data provenance), and data privacy (including data anonymization, encryption, and access control) [19]. For instance, considering big data in healthcare, it is crucial to protect sensitive patient data especially when dealing with privacy and security issues. Additionally, in [16] it was illustrated the distinctions between privacy and security issues that arise when dealing with big data, in which the primary security objective is to safeguard the information and not adequate to address privacy issues. In their research, they explain that, while privacy was more dependent on individual management of data (implementing policies to ensure that customer data was being gathered, used, and shared appropriately), security was more concerned with the protection of the data from malicious attacks and acquiring profit from the stolen data.

Data interoperability across primary and secondary healthcare systems was essential for the improvement of the end-user experience when discussing the national eHealth information system. To make it easier to integrate and share data between several platforms, it was crucial to develop common technological standards for data interchange between the primary and secondary healthcare systems. Adoption of common standards could be considered for this purpose, such as DICOM [20] (Digital Imaging and Communications in Medicine), SNOMED CT [21] (designed as a multilingual international core set for electronic clinical data exchange that can be used in Electronic Health Records (HER) systems), and HL7 FHIR [22] (next-generation standard for interoperability developed by Fast Healthcare Interoperability Resources and Health Level 7 to provide efficient and quick health data exchange) [23].

The sensitive patient data that must be legally protected and secured raised concerns when dealing with eHealth systems that monitor all the patient information and data as well as the medical staff who provide healthcare. According to WHO in [14], over 80% of the EU member states have created laws to protect the privacy of sensitive health information, which almost 30% from 2009 to 2016 was raised exponentially. Furthermore, the medical personnel must address additional challenges related to financial difficulties, computer expertise, information technology support, etc. when implementing eHealth systems [24]. In [25] it was pointed out that eHealth systems must have strong privacy and security policies in place to be able to handle these issues. The medical practitioners as the major users of these health systems must be aware of and abide by the established security procedures to reduce the threats associated with the digital transfer and storage of medical data [26].

The dynamic nature of security and privacy in healthcare was highlighted in [27], who additionally point out the significance of current security practice reviews and observation in order to respond to emerging vulnerabilities and threats. The medical staff members must take part in frequent education and awareness

programs in order to be informed about the latest security requirements and best practices. In [28] the focus was put on privacy and security concerns in the era of digital healthcare, emphasizing the need for robust security protocols to manage the issues and challenges posed by the rapid advancements of technology and the expanding amount of data in the healthcare sector. A question was posed on privacy protection and sensitive information, addressing the national data protection laws and the General Data Protection Regulation (GDPR). The topic of discussion was "Is it decently implemented in the medical field?". As a member of the Council of Europe since 2006, N. Macedonia has benefited from the creation of the Convention for Protection of Individuals related to the Automatic Processing of Personal Data, known as Convention 108, and on December 5th, 2019, was made the 37th nation to sign the updated Convention 108+ [29, 30]. The two main objectives of this revised Convention 108+ were to effectively reinforce the Convention's execution and address different issues that may arise from employing the new Information and communication technology. According to the convention, member nations must ensure that the individuals are informed about which and what type of information was being gathered about them, have access to the data, and can make corrections to their data. To keep up with the EU's GDPR, the new law on personal data protection was passed by Macedonian Parliament that went into effect in February 2020 [31, 32]. This law establishes responsibilities for the data processors and controllers to respect and safeguard the individuals' right to privacy. Also, this law regulates the processing of sensitive health information as personal data.

The opinion of the medical practitioners on eHealth technology security and privacy safeguards was the focus of this study. Their familiarity with the security mechanisms in place was evaluated, and possible areas of improvement – specifically, with the "Moj Termin" (My Appointment) system currently operational in N. Macedonia were highlighted. Understanding these problems would enable recommendations to be made to strengthen privacy of patient data and enhance the system's performance. To investigate these privacy and security concerns, the medical practitioners were subjected to a comprehensive email interview and a structured survey to evaluate their awareness of the security protocols and opinions regarding the protection of private medical information. By focusing on the system "Moj Termin", the results from the survey will be used to provide guided suggestions for enhancing the overall security and privacy of health care information systems.

The remaining sections of this research are arranged as follows: The study's tools and methods were detailed in the Materials and Methods section. The Results section includes the study's findings. The Discussion section interprets the survey and interview data and highlights the important findings. The conclusion section summarizes the findings of this research and offers recommendations for the medical authorities, organizations, and various IT bodies, emphasizing the value of providing ongoing education and training for medical practitioners to familiarize them with various privacy and security measures.

2. Materials and Methods

To gain a better grasp of the effect that using eHealth information systems has on the medical practitioners' awareness of the security and privacy of sensitive medical data, indebted e-mail interviews were the initial method used to conduct this research. The e-mail interviews presented an excellent alternative to phone and in-person interviews. Furthermore, the participants who were difficult to get in touch with lived in distant locations, or just didn't have the time because of their jobs may benefit more from this kind of qualitative research [33, 34]. The primary problem with this approach was that, in many cases, the interview participants weren't responsive to their requests to take part in the interview. To avoid this challenge, timed reminders were necessary [33].

Before conducting the e-mail interviews, a set of materials was put together, which included interview questions, a completed and scanned interview permission form, interview instructions, and an invitation to the interview by e-mail. Finally, there were no financial incentives offered as rewards to the study's participants.

The focus of this research was the addressed questions about security and privacy measures of sensitive medical data and the viewpoints of the participants in the context of challenges and difficulties. These questions included:

- What security measures were available to you while handling sensitive eHealth information belonging to the patients?
- What kinds of issues did you encounter when utilizing the eHealth information system "Moj Termin"?
- What features, data, services, etc. do you believe the eHealth information system "Moj Termin" requires?
- How did the administrators of the medical department help you when you first started using this information system "Moj Termin"?
- Which security measures were disposal to you when handling the sensitive data belonging to the patients?

The Interview transcripts were examined, and the questions were reviewed. The data was evaluated and examined to uncover similar statements on issues and concerns related to security and privacy.

An online survey was used in the second technique of this study to include a considerably bigger number of participants for the research relevance and further investigation of the topic at hand. Only the first section of the questionnaire, which included the demographic characteristics of physicians of primary and secondary level, and the third section, which included the issues and challenges were taken into consideration for this study out of the total six sections that the questionnaire was composed of.

Survey of primary and secondary physicians was carried out in N. Macedonia in two-months, between February 7th and April 7th, 2022. Considering the physicians' busy schedules, closed hospitals except in cases of emergency, and the reason that many of them were ill and isolated at home, the medical personnel were difficult to contact during the COVID-19 outbreak.

2.1. Study population

The standardized formula for minimal sample size was used to estimate the minimal sample size for this study to be relevant and achieve its primary goal [35].

$$n = \frac{\frac{z^2\pi(1-\pi)}{e^2}}{1 + \frac{z^2\pi(1-\pi)}{e^2 N}} \quad (1)$$

The formula considers the following factors:

- Sample size (n),
- Population proportion (π),
- Desired confidence level (z),
- Acceptable sampling error (e), and
- Population size (N).

At the time of access, in N. Macedonia were registered 4636 specialists in outpatient clinics, 1793 pharmacists, 1554 general physicians, and 160 gynecologists [36].

Based on the 9386 total population, 370 participants were necessary according to (1) to complete the questionnaire for the study to be relevant with a 95% confidence level and a 5% margin of error. All medical practitioners who worked with or had knowledge of the eHealth system "Moj Termin" usage were eligible to participate in this study. The technical workers at the healthcare facilities, those who had never utilized the eHealth system, and those who had not given informed consent were excluded from the study.

2.2. Statistical analysis

IBM SPSS Statistics version 23.0, a statistical program for the Windows operating system was utilized to examine the collected data [37]. The data analysis's categorical variables were provided as frequencies and percentages. To find any significant link between the variables, a cross-tabulation was performed. Phi and Cramer's V were utilized for calculation of the effect size between the variables, and to test the correlation, the Chi-Square test was used. A two-tailed p-value < 0,05 was considered significant and for the null hypothesis, it was assumed that there would be no relationship between the variables.

3. Results

3.1. Participants' demographic characteristics

3.1.1. Results from in-depth interviews

Between April and September 2020, the study's participants began to receive invitations for interviews, out of which, eight medical practitioners took part in the study (five being primary and three secondary care physicians). The demographic details of those who took part in the interview procedure are displayed in Table 1. They all finished the email interview, and two of them additionally had a follow-up email exchange. The interviews lasted between 20 to 40 minutes (on average) and it took the physicians one to two weeks (8,25 days on average) to respond after they received the invitation.

Table 1: Demographic characteristics of medical practitioners from the in-depth interviews

Characteristics	
Gender – No. (%)	
Male	1 (12,5%)
Female	7 (87,5%)
Age, years – Mean (±SD)	33,8 (±10,5)
Level of Education – No. (%)	
University	6 (75%)
PhD	1 (12,5%)
Other	1 (12,5%)
Profession – No. (%)	
Primary healthcare physician	5 (62,5%)
Specialist	3 (37,5%)
Work experience of primary healthcare physician, years – Mean (±SD)	7,8 (±10,3)
Work experience of specialist, years – Mean (±SD)	5,7 (±4,1)
Experience in patient management before starting to use the eHealth system – No. (%)	3 (37,5%)
No experience in patient management before starting to use the eHealth system – No. (%)	5 (62,5%)

3.1.2. Results from the online survey

As shown in Figure 1, most of the participants who took part in the online survey were from primary healthcare.

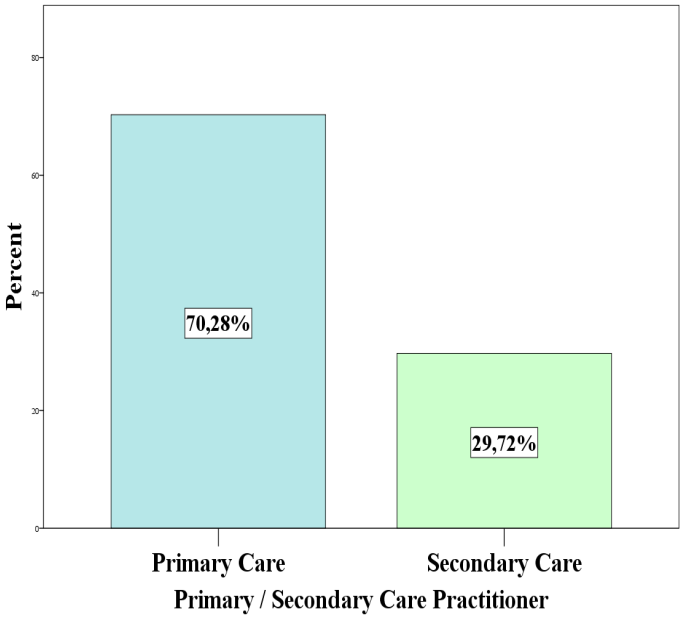

Figure 1: Medical practitioners' distribution within the healthcare sectors

The majority of the medical practitioners who took part in this survey were female, married, and had finished their specialty training as presented in Table 2. Furthermore, it was estimated that the typical medical practitioner had 19 (+/-10,5) years of overall work experience, however, the average years of experience with the eHealth system were estimated to be 7,5 (+/-3,8) years. Finally,

as shown in Table 2, most of the participants worked in an urbanized environment.

Table 2: Results from the online survey - Demographic characteristics of medical practitioners

Characteristics	
Age, in years – Mean (±SD)	46,9 (±10,9)
Gender – N (%)	
Female	244 (66,1)
Male	125 (33,9)
Marital status – No. (%)	
Married	314 (84,9)
Unmarried	37 (10,0)
Widowed	17 (4,6)
Other	2 (0,5)
Education – N (%)	
Specialized studies	206 (56,4)
Graduate	123 (33,7)
PhD	19 (5,2)
Postgraduate	16 (4,4)
Other	1 (0,3)
Practitioners' Healthcare Sector – N (%)	
Primary Care	253 (70,3)
Secondary Care	107 (29,7)
Working experience of the medical practitioner, in years – Mean (±SD)	19,1 (±10,5)
Location of the medical facility – N (%)	
Urban Area	321 (87,2)
Rural Area	47 (12,8)
eHealth system patient management experience, in years – Mean (±SD)	7,5 (±3,8)

The distribution of the participants was approximately evenly distributed, with the majority falling within the age range of 28 and 62, as seen in Figure 2.

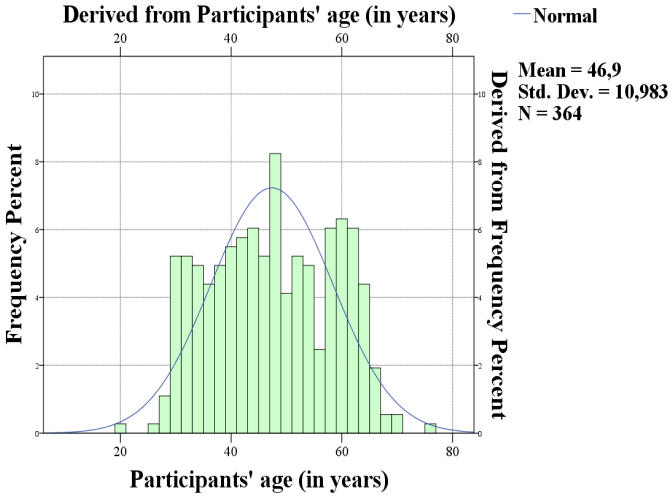

Figure 2: Results from the online survey - Age distribution of the medical practitioners

The specializations of the medical practitioners included in this analysis are shown in Table 3. Of these, the majority were registered as other specialized physicians, followed by general practitioners, and dentists.

Table 3: Medical practitioners' area of expertise

Physician's role		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Gynecologist	21	5,7	6,1	6,1
	Dermatologist	2	,5	,6	6,7
	Dermatologist and venereologist	2	,5	,6	7,3
	Internist	14	3,8	4,1	11,4
	Effectologist	4	1,1	1,2	12,5
	Clinical pharmacologist	1	,3	,3	12,8
	Maxillofacial surgeon	1	,3	,3	13,1
	Neurologist	3	,8	,9	14,0
	Neuropsychiatrist	1	,3	,3	14,3
	Neurosurgeon	1	,3	,3	14,6
	Nuclear medicine	2	,5	,6	15,2
	General Medicine	66	17,8	19,2	34,4
	Orthopedist	3	,8	,9	35,3
	Otorhinolaryngologist	8	2,2	2,3	37,6
	Ophthalmologist	3	,8	,9	38,5
	Pediatrician	21	5,7	6,1	44,6
	Pneumophthisiologist	1	,3	,3	44,9
	Psychiatrist	2	,5	,6	45,5
	Radiologist	2	,5	,6	46,1
	X-ray specialist	1	,3	,3	46,4
	Social medicine	4	1,1	1,2	47,5
	Specialist	13	3,5	3,8	51,3
	Sports medicine	1	,3	,3	51,6
	Dentistry	58	15,7	16,9	68,5
	Transfusiologist	2	,5	,6	69,1
	Urologist	3	,8	,9	70,0
	Physical medicine and rehabilitation	7	1,9	2,0	72,0
	Surgeon - Specialist	5	1,4	1,5	73,5
	Other specialist doctors	91	24,6	26,5	100,0
	Total	343	92,7	100,0	
Missing		27	7,3		
Total		370	100,0		

3.2. Challenges and Issues (Contextual Aspects)

The opinions of the medical practitioners on the challenges and issues they encountered when utilizing the eHealth system are shown in Table 4. The majority of the medical practitioners in this survey reported that throughout their working experience in the eHealth system, they occasionally ran across different persistent technical challenges, nevertheless, this group was closely followed by those who often faced consistent issues. When faced with various technical issues, the majority of the medical practitioners stated they were rarely given assistance or some technical support by the medical authorities. However, 16,1% stated they never received any assistance or support from medical authorities. When the medical practitioners first began using the eHealth information system, the majority of them did not received introduction or explanation of the security and privacy measures that were implemented to protect the sensitive patient medical data and information that was being stored in the eHealth information system. Lastly, the majority of the medical practitioners in this study strongly agreed that the information system required a variety of significant and critical enhancements to the system functionalities. These system functionalities are to be integrated and upgraded to the current implementation based on their working experience with the system and its effectiveness in managing patients.

Table 4: Medical practitioners' opinions on challenges and issues in utilizing the eHealth information system

Context Factors	N (%)
Frequently run into recurring technical issues when using the eHealth system	
Always	54 (14,6)
Very often	123 (33,3)
Sometimes	133 (36,0)
Rarely	48 (13,0)
Never	11 (3,0)
Frequently got assistance or technical support from the medical authorities when faced with technical difficulties	
Always	46 (12,5)
Very often	74 (20,2)
Sometimes	91 (24,8)
Rarely	97 (26,4)
Never	59 (16,1)
Presented with different privacy and security measures to safeguard the patients' sensitive medical data stored in the eHealth system	
To a great extent	53 (14,4)
Somewhat	93 (25,3)
Very little	89 (24,3)
Not at all	132 (36,0)
Significant functional improvements are required for the eHealth system	
Strongly agree	210 (56,9)
Agree	82 (22,2)
Undecided	60 (16,3)
Disagree	14 (3,8)
Strongly disagree	3 (0,8)

Figure 3 presents an introduction to the various security measures implemented concerning the security and privacy protection of the patient's sensitive medical data by the practitioners' gender, distribution within the healthcare sectors, and the location of their medical facility.

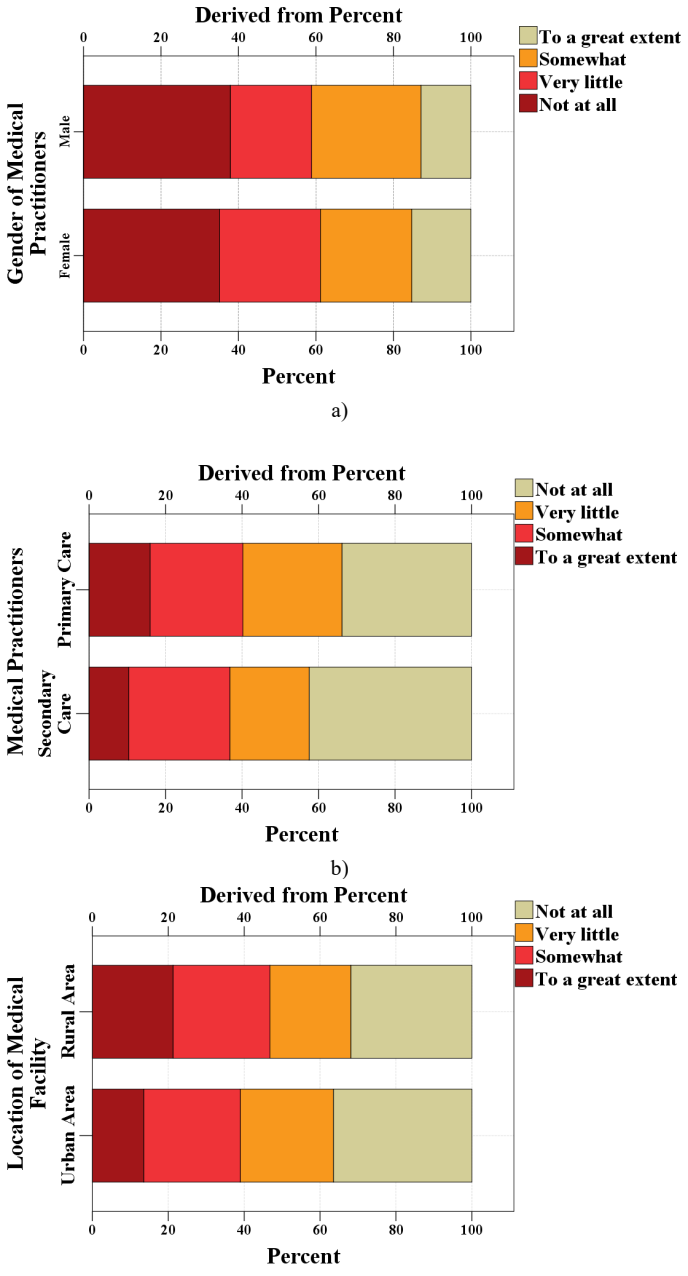

Figure 3: Various privacy and security measures in relation to protecting patients' sensitive medical data presented by a) Practitioners' gender; b) Distribution within the healthcare sectors; and c) Location of their medical facility

A crosstabulation between the variables presented various security measures to safeguard the patients' sensitive medical data stored in the system and often receives technical support and assistance when encountering technical difficulties while working in the system is presented in Table 5. A greater number of the medical practitioners than anticipated did not receive any assistance or support from the medical authorities, nor were they informed of the numerous privacy and security procedures

implemented to safeguard patients' private medical information. The number of medical practitioners who occasionally, frequently, and consistently received assistance and support from the medical authorities was lower than anticipated. Additionally, there was a complete lack of introduction of security protocols regarding the safeguarding of patients' sensitive medical data.

Table 5. Crosstabulation of the variables Often receive assistance and technical support from the medical authorities and Presented with various privacy and security measures

Frequently got assistance or technical support from the medical authorities when faced with technical difficulties		Presented with different privacy and security measures to safeguard the patients' sensitive medical data stored in the eHealth system				
		Not at all	Very little	Somewhat	To a great extent	Total
Never	Count	32	12	6	9	59
	Expected Count	21,2	14,4	15,1	8,3	59,0
Rarely	Count	39	28	23	6	96
	Expected Count	34,5	23,5	24,5	13,5	96,0
Sometimes	Count	28	25	30	7	90
	Expected Count	32,4	22,0	23,0	12,6	90,0
Very often	Count	18	20	24	11	73
	Expected Count	26,3	17,8	18,7	10,2	73,0
Always	Count	14	4	10	18	46
	Expected Count	16,6	11,2	11,8	6,4	46,0
Total	Count	131	89	93	51	364
	Expected Count	131,0	89,0	93,0	51,0	364,0

Certain medical practitioners were somewhat introduced with different security and privacy preferences taken in regard to protecting the patients' sensitive data, however, they never, rarely, or always received any aid and support from the medical authorities when was required. There were more medical practitioners who sometimes and frequently got assistance and support from the medical authorities than expected. They were somewhat introduced to different privacy and security measures that were taken in relation to protecting the sensitive patients' data.

There were certain medical practitioners who rarely and sometimes received assistance and support from the medical authorities than to be expected, that to a great extent were introduced to different privacy and security measures taken in relation to protecting the sensitive patients' medical data. There were more medical practitioners who never, frequently, and always received assistance and support from the medical authorities than to be expected, that to a great extent were introduced with different privacy and security measures taken in relation to protecting the sensitive patients' medical data.

There was a statistically significant difference (X^2=53,194, p=0,000) between the opinions that introduction to different privacy and security measures to safeguard the sensitive medical data of the patients and often received assistance and support from the medical authorities. Since the p-value in this instance was less than the alpha standard value of 0,05, the null hypothesis, which stated that the two variables were independent of each other was rejected. The data indicates that the variables' introduction to different privacy and security measures for the protection of the sensitive data of the patients and frequently receiving assistance and support from the medical authorities were related to one another. The effect of this association was almost moderate (0,221), meaning that the assistance provided by the medical authorities may have had some role in the way in which the medical practitioners answered the given questions. The remaining variables, such as age group, marital status, location of the medical facility, education, gender, employment history, etc., did not reveal any significance of impact on the opinions of the medical practitioners.

4. Discussion

The in-depth interviews and online surveys were the two main research methodologies used in this study to examine the difficulties and concerns related to privacy and security when handling the sensitive information of the patients. The fact that a wide range of medical practitioners with different specialties (Table 3) offered their opinions on the use of the eHealth information system enhanced the level of quality and importance of this research. The government and medical authorities have the responsibility of authorizing the adoption of these eHealth systems without giving any thought to the security integrity of the private medical data of the patients [38]. For comparable eHealth information systems in other developing nations, this study would likewise present relevant data and support the government leaders and medical authorities.

This study was carried out among primary and secondary care practitioners (Table 3) to find out what they thought of the privacy and security features of the system, what was lacking, and what features and services should be enhanced to provide patients with better treatment. The answers to the survey revealed that the experiences of the medical practitioners with the security measures implemented by the medical authorities varied greatly. A significant portion of the survey participants, who believed that the different privacy and security measures were not sufficiently introduced and presented to them, emphasized the needs for improving the awareness and training programs to be initiated more frequently (Table 4). By filling in these knowledge gaps with different training and seminars, the healthcare authorities should ensure that the medical practitioners have the skills required to safeguard and protect the patient's sensitive data and respect the privacy and protection legislation [39].

Data interoperability requirements and protecting the privacy and security of sensitive patient medical data are potential challenges when working with external documents associated with

medical data exchange between primary and secondary care. It may be challenging to integrate the patients' medical data records or other healthcare-related documents into the broader eHealth system since they may be kept in several external systems at various locations. To address this challenge and issue with interoperability, appropriate funding is required for collaboration with external systems and data integration technologies to ensure operational sharing of medical sensitive data. As was already indicated, an additional difficulty was guaranteeing the privacy and security of the patient's medical data because, the system holds the personal data of the patients, such as their insurance information and medical history. Considering this, these various healthcare systems need to implement the necessary safeguards to protect sensitive data from unauthorized access and cyber threats [23].

As an example, across the user experience of patients, medical practitioners, and other end-users may have greatly impacted to the integration of privacy and security measures in the national eHealth information systems. From one perspective, robust security and privacy measures may enhance the trust in the healthcare system and the end-user confidence by providing reassurance that their private medical information is being shielded from unwanted access, disclosure, and use. This would improve the overall user experience as they would be more likely to feel content and at ease in using the eHealth system and its features. On the other hand, inadequate privacy and security measures may lead to unfavorable user experiences because the end-users could be concerned that their private medical information which must remain confidential with implemented safeguards may be compromised or that too strict safety measures would make it impossible for them to access or share their data. This could cause distrust, annoyance, and a reluctance to utilize the eHealth information system [23, 39].

The Law on Health Protection includes regulations for the security of patient data specifically for the healthcare industry. Because of this, the health data is regarded as sensitive information and is given extra protection under Macedonian law. However, there may be several obstacles to effectively implementing and enforcing these regulations and laws in day-to-day life, not just in N. Macedonia, but in any other country. The Macedonian healthcare practitioners must understand their responsibilities under the data privacy laws and take the appropriate safety measures to safeguard the patient's sensitive medical data. The EU has regulations in place to protect individuals' rights when it comes to the gathering and usage of personal sensitive data. These regulations include the General Data Protection Regulation (GDPR) and the Directive on the Protection of Individuals concerning the processing of personal data by adequate authorities, both of which have as their main objectives the prevention, investigation, detection, prosecution, or the implementation of penalties for criminal offenses. For these reasons, all nations, especially N. Macedonia, must ensure that the right policies are implemented to safeguard the rights of the population and that they always remember the ethical principles when handling medical data It meant guarantee that the data was being collected and used openly, that sufficient organizational and technical security measures were being put in place, and that people's consent was being appropriately requested. To ensure that people are not treated unfairly in light of the findings of big data analysis, it was also crucial to address concerns of prejudice and discrimination when analyzing the medical data [29, 30, 31, 32].

This study also assessed the perceptions of medical practitioners on the functionality of the eHealth information system. This was crucial since system updates could enhance both the user experience and the overall security of the system (Table 4). By concentrating on the precise areas where the medical practitioners believe that improvements are necessary, the IT staff can focus their efforts on resolving these issues and with that offering better security measures.

This research adds to the amount of knowledge already available on privacy and security issues in healthcare systems especially in medical information systems. It aligns with the increased focus on patient privacy, data security, and compliance with legal frameworks such as the GDPR and the Health Insurance Portability and Accountability Act (HIPPA). Enhancing the security and privacy of eHealth systems is imperative, so it's crucial to identify useful insights the parties involved may apply to improve eHealth systems [40].

This study has its limitations because it concentrated on the use of the "Moj Termin" eHealth information system that is currently in use in N. Macedonia. Second, there was a lack of a straightforward open discussion between the interviewer and the participants because the in-depth interviews were conducted remotely via e-mail. Thirdly, the online survey sample utilized in this study was restricted to only Macedonian healthcare professionals working in primary and secondary healthcare level, as such, it may not accurately reflect the majority of medical practitioners both inside and outside the nation. Thus, more research is required to examine the boundaries of the various eHealth systems in use in other more developed countries, as well as to find out what many relevant medical and technical professionals think about the issue at hand, which directions should be pursued, and how to provide further upgrades for the eHealth systems to develop properly.

5. Conclusion

The study's findings demonstrate the urgent need for better security and privacy safeguards when medical practitioners utilize the eHealth systems. The healthcare authorities and IT companies must act quickly in response to the recognized difficulties with the eHealth systems, the lack of expertise and knowledge of the current security and privacy standards. By resolving these issues, medical practitioners' confidence in the security of protecting private patient information could be increased. This will eventually aid in the successful integration of the eHealth system technology into the delivery of overall healthcare.

Integrating privacy and security safeguards into the national healthcare and medical information systems may have a substantial impact on how patients, medical practitioners, and other end-users interact with the system. Users would therefore likely feel more satisfied and comfortable utilizing the eHealth information system and its features, which would enhance the user experience. Inadequate privacy and security measures, however, may have the opposite negative effect. End-users may worry that their personal medical data won't be secure, that the security measures in place will be compromised, or that they won't be able

to access or share their data easily because of overly strict regulations and security measures. This could cause mistrust, reluctance, and annoyance to utilize the eHealth system. In consideration of this, integrating sufficient security and privacy features into the system would be essential to maintaining the confidence of the patients. It's also essential to implement this under the relevant regulations. Privacy and security measures should be included in the design and implementation of eHealth systems in a way that creates a balance between the need for data protection, usability and accessibility. The following are some suggestions for a user-centered integration of security and privacy safeguards into national medical information systems, as well as for presenting these ideas as a kind of implementation roadmap: Start a user research project and utilize the results to assist the medical organization in better understanding the user requirements, expectations, and preferences regarding privacy and security safeguards that are in line with those demands; Healthcare organization should involve the users in the design process of privacy and security measures. Through user testing and other feedback sessions, they can ensure that the implemented measures are clear, in line with expectations and requirements, and easy to use; Provide users with accurate and transparent information about the privacy and security safeguards implemented through data usage agreements and privacy policies. This would increase users' trust in the system and increase their level of satisfaction in general; User-friendly authentication techniques, like single log-in or biometric authentication, to provide users with easier, secure system access; and finally, monitor and assess the effectiveness of the privacy and security safeguards that have been put in place to make any necessary adjustments along the road to ensure that they continue to fulfill the requirements and expectations of the end-users.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] V. Denkovski, I. Stojmenovska, G. Gavrilov, V. Radevski, V. Trajkovik, "Investigating Privacy and Security Concerns in a Running eHealth Information System," in 2023 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), 39-44, 2023, doi:10.1109/MeditCom58224.2023.10266398.

[2] T. O. Abolade, "The benefits and challenges of e-Health applications in developing nations: A review," in 14th iSTEAMS Conference, 14, 37-44, 2018.

[3] B. Atanasovski, M. Bogdanovic, G. Velinov, L. Stoimenov, D. Sahpaski, I. Skrceska, M. Kon-Popovska, D. Jankovic, B. Jakimovski, "Transforming an Enterprise E-Health Syste,m from Process Oriented to Model Driven Architecture," in 7th International Conference on Information Society and Technology ICIST, 159-162, 2021.

[4] S. Olsson, A. Lymberis, D. Whitehouse, "European Commission activities in eHealth", International Journal of Circumpolar Health, **63**(4), 310–316, 2004, doi:10.3402/ijch.v63i4.17747.

[5] P. G. Svensson, "eHealth Applications in Health Care Management," Ehealth international, 1(1), 5, 2002, doi:10.1186/1476-3591-1-5.

[6] S. Faber, M. van Geenhuizen, M. de Reuver, "eHealth adoption factors in medical hospitals: A focus on the Netherlands," International journal of medical informatics, 100, 77–89, 2017, doi:10.1016/j.ijmedinf.2017.01.009.

[7] R. Mitrovska, V. Pachovski, A. Bozinovski, "Challenges, benefits and expectations from implementing an e-health system in Macedonia," in 2015 Proceedings of the 12th International Conference on Informatics and Information Technologies (CiiT 2015), 268-272, 2015.

[8] G. Dussault, L. Lapão, "The contribution of ehealth and mhealth to improving the performance of the health workforce: a review," Public Health Panorama, 3(3), 463-471, 2017.

[9] A. La Rocca, T. Hoholm, "Coordination between primary and secondary care: the role of electronic messages and economic incentives," BMC Health Serv Res 17, 149, 2017, doi: 10.1186/s12913-017-2096-4.

[10] R. A. Tariq, P.B. Hackert, "Patient Confidentiality", in StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing, 2023, Available from: https://www.ncbi.nlm.nih.gov/books/NBK519540/, [Last Accessed: January 3, 2024].

[11] S. Khanra, A. Dhir, A.K.M.N. Islam, M. Mäntymäki, "Big data analytics in healthcare: a systematic literature review", Enterprise Information Systems, 14(7), 878–912, 2020, doi: 10.1080/17517575.2020.1812005.

[12] S. Kumar, M. Singh, "Big data analytics for healthcare industry: impact, applications, and tools", Big Data Mining and Analytics, 2(1), 48–57, 2019, doi: 10.26599/BDMA.2018.9020031.

[13] European Commission, "Exchange of Electronic Health Records across the EU", Shaping Europe's digital future, Policy, 2021, Available from: https://ec.europa.eu/digital-single-market/en/exchange-electronic-health-records-across-eu#:~:text=The%20eHDSI%20connects%20eHealth%20national,such%20health%20information%20by%202021, [Last Accessed: January 3, 2024].

[14] World Health Organization Regional Office for Europe, "From innovation to implementation eHealth in the WHO European Region", WHO Regional Office for Europe, 2016, Available from: https://intranet.euro.who.int/__data/assets/pdf_file/0012/302331/From-Innovation-to-Implementation-eHealth-Report-EU.pdf, [Last Accessed: January 3, 2024].

[15] T. Yuan, "Towards the development of best data security for big data", Communications and Network, 9(4), 291-301, 2017, doi: 10.4236/cn.2017.94020.

[16] P. Jain, M. Gyanchandani, N. Khare, "Big data privacy: a technological perspective and review", Journal of Big Data, 3(1), 25, 2016, doi: 10.1186/s40537-016-0059-y.

[17] U. Sivarajah, M.M. Kamal, Z. Irani, V. Weerakkody, "Critical analysis of big data challenges and analytical methods", Journal of Business Research, 70, 263–286, 2017, doi: 10.1016/j.jbusres.2016.08.001.

[18] A. Oussous, F.Z. Benjelloun, A. Ait Lahcen, S. Belfkih, "Big data technologies: A survey", Journal of King Saud University - Computer and Information Sciences, 30(4), 431-448, 2017, doi: 10.1016/j.jksuci.2017.06.001.

[19] H. Ye, X. Cheng, M. Yuan, L. Xu, J. Gao, C. Cheng, "A survey of security and privacy in big data", in 2016 16th International Symposium on Communications and Information Technologies (ISCIT), 268-272, 2016.

[20] The Medical Imaging Technology Association (MITA), "DICOM® — Digital Imaging and Communications in Medicine", 2024, Available from: https://www.dicomstandard.org/, [Last Accessed: January 4, 2024].

[21] The National Library of Medicine, "SNOMED CT a standard for electronic exchange of clinical health information", 2024, Available from: https://www.nlm.nih.gov/healthit/snomedct/index.html, [Last Accessed: January 4, 2024]

[22] The FHIR Core Work Group, "FHIR ®© HL7.org 2011+. FHIR R5 hl7.fhir.core#5.0.0", 2024, Available from: https://hl7.org/fhir/overview.html, [Last Accessed: January 4, 2024].

[23] A. Torab-Miandoab, T. Samad-Soltani, A. Jodati, P. Rezaei-Hachesu, "Interoperability of heterogeneous health information systems: a systematic literature review", BMC medical informatics and decision making, 23(1), 18, doi:10.1186/s12911-023-02115-5.

[24] I. Khan, G. Xitong, Z. Ahmad, F. Shahzad, "Investigating factors impelling the adoption of e-Health: A perspective of African expats in China," SAGE Open, 9(3), 2019, doi: 10.1177/2158244019865.

[25] A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar, R. A. Khan, "Healthcare Data Breaches: Insights and Implications," Healthcare (Basel, Switzerland), 8(2), 133, 2020, doi:10.3390/healthcare8020133.

[26] D. El Majdoubi, H. El Bakkali, S. Sadki, Z. Maqour, A. Leghmid, "The systematic literature review of privacy-preserving solutions in smart healthcare environment," Security and Communication Networks, 1–26, 2022, doi:10.1155/2022/5642026.

[27] M. Javaid, A. Haleem, R. P. Singh, R. Suman, "Towards insighting cybersecurity for Healthcare Domains: A comprehensive review of recent practices and Trends," Cyber Security and Applications, 1, 2023, doi:10.1016/j.csa.2023.100016.

[28] M. Pyrrho, L. Cambraia, V. F. de Vasconcelos, "Privacy and Health Practices in the Digital Age", The American journal of bioethics : AJOB, 22(7), 50–59, 2022, doi:10.1080/15265161.2022.2040648.

[29] Council of Europe, "Convention 108+ Convention for the protection of individuals with regard to the processing of personal data", 2018, Available from: https://coe.int/en/web/data-protection/convention108-and-protocol, [Last Accessed: January 4, 2024].

[30] Council of Europe, "Modernization of convention 108 - data protection -", 2024, Availabe from: https://www.coe.int/en/web/data-protection/convention108/modernised, [Last Accessed: January 4, 2024].

[31] Official Gazette of the Republic of North Macedonia no. 42/20 and 294/21, "DP Law", 2020, [Last Accessed: January 4, 2024].

[32] DLA PIPER., "Data Protection Laws of the World North Macedonia", 2022, Available from: https://www.dlapiperdataprotection.com/index.html?t=law&c=MK#:~:text=The%20DP%20Law%20defines%20personal,his%20or%20her%20personal%20identification, [Last Accessed: January 4, 2024].

[33] J. E. Hawkins, "The practical utility and suitability of email interviews in qualitative research," The Qualitative Report, 23(2), 493-501, 2018, doi: 10.46743/2160-3715/2018.3266.

[34] R. L. Fritz, R. Vandermause, "Data collection via in-depth email interviewing: Lessons from the field," Qualitative Health Research, 28(10), 1640–1649, 2018, doi: 10.1177/1049732316689067.

[35] D. M. Levine, D. F. Stephan, A. S. Kathryn, Statistics for managers: Using Microsoft excel, 9th edition, Pearson, 2018.

[36] Health Insurance Fund of Republic of North Macedonia, "Code of physicians", 2022, Available from: https://fzo.org.mk/en/node/1126, [Last Accessed: January 4, 2024].

[37] SPSS Inc., "IBM SPSS Statistics", 2023, Available from https://www.ibm.com/products/spss-statistics, [Last Accessed: January 4, 2024].

[38] H. C. Ossebaard, L. Van Gemert-Pijnen, "eHealth and quality in health care: implementation time," International journal for quality in health care: journal of the International Society for Quality in Health Care, 28(3), 415–419, 2016, doi:10.1093/intqhc/mzw032.

[39] A.T. Alanazi, "Clinicians' Perspectives on Healthcare Cybersecurity and Cyber Threats", Cureus, 14, 15(10), e47026, 2023, doi: 10.7759/cureus.47026.

[40] P. Yamcharoen, O. S. Folorunsho, A. Bayewu, O. E. Fatoye, "Advancing Healthcare Security: Developing a Composite Set of Cybersecurity Requirements for the Healthcare Industry", Computing, Information Systems, Development Informatics & Allied Research Journal, 14(1), 9-20, 2023, doi: 10.22624/AIMS/CISDI/V14N1P2.