Engineering Applications

https://publish.mersin.edu.tr/index.php/enap

e-ISSN 2979-9201

How secure is our medical data? Is Albania ready for the digitalization of the health care system?

Dolantina Hyka [*1], **Fatmir Basholli** [2]

[1]*Mediterranean University of Albania, Department of Information Technology, Albania, dolantina.hyka@umsh.edu.al*
[2]*Albanian University, Department of Engineering, Tirana, Albania, fatmir.basholli@albanianuniversity.edu.al*

Cite this study: Hyka, D., & Basholli, F. (2023). How secure is our medical data? Is Albania ready for the digitalization of the health care system?. Engineering Applications, 2 (3), 235-242

Keywords
CyberSecurity
Information Security
Health Care
Cryptosystems
Privacy

Research Article
Received:28.03.2023
Revised: 01.09.2023
Accepted:19.09.2023
Published:26.09.2023

Abstract

Managing safety in the health system is important as connections between external clients of hospital systems need to be carefully managed. It is often thought that public health institutions do not need structured information security, as they are not part of a competitive environment and tend to have more simplified IT infrastructure, as most information systems are for internal use and therefore, they are less exposed to external threats. However, this is no longer true. Public health institutions have very sensitive information, they also store confidential information about individuals, thus making them possible targets for many hackers. This paper aims to study information security in detail by analyzing information security practices in hospitals. Managing safety in the health system is important because the health system through the systems it uses and the services it provides has the personal data of the entire population of a country. It is therefore very important that connections between external clients of health systems are carefully managed. As this information stored in these systems can cause image damage to certain individuals, but can also interfere with changing dates, causing damage to people's lives. This information is very sensitive for some people and their security is primary.

1. Introduction

The purpose of this paper is to analyze information security practices in Albanian public and private hospitals, in order to determine the level of Information Security in this sector, and to provide suggestions for improvements and also to analyze the state of information security in Albanian public institutions by providing a clearer picture of the level of development of information security and the steps that need to be taken to further advance.

The entire public and private health system through the systems they use and the services they provide are the users and, in a sense, also the owners of personal data of the entire population of a country. They contain very important information in electronic version that should be protected from serious threats which may be abuse as well as illegal actions with the data, but also their destruction. The rapid development of information-threatening techniques poses a serious risk to information. Developing and managing ongoing protection is necessary to keep information as secure as possible.

For users of information systems, it is important to ensure the security of their data whether personal or not. It is therefore essential that users have a good knowledge and awareness of information security practices based on regulations, policies and practices. This study will reflect the state of this documentation in the health system and provide suggestions on how improvements can be made.

This study helps healthcare leaders reduce hospital sensitivity by detailing the results that come from strategic online safety development decisions. It also helps cyber security professionals to understand the complexities of developing internet security capability in hospitals. In this rapidly changing and evolving environment, information as a valuable asset is always under threat.

Internal policy: they deal with the same internal policy that other large organizations do, but complicated by the complexity of the functions involved within the organization: finance, IT, and human resources, just like other organizations; unlike other organizations, they should also support radiology, cardiology and pediatrics among others. The degree of specialization is high. Each department requires completely different equipment, meets different patient needs, has different workflows, and employs a highly specialized workforce that takes years to train. Regulatory pressures: similar to other organizations, they must abide by the regulations imposed on them by the state and the federal government; but in the United States, health care records are considered to be particularly sensitive, and thus, protected under additional specific data protection laws. Patient-Centered Care: Like all organizations in the United States, hospitals care about their ability to generate positive net income for survival, but unlike other organizations, their first mission is to care for their patients, even when they are profitable. This study helps healthcare leaders reduce hospital sensitivity by detailing the results that come from strategic online safety development decisions. It also helps cyber security professionals to understand the complexities of developing internet security capability in hospitals. In this rapidly changing and evolving environment, information as a valuable asset is always under threat. Based on the literature, there are more than twelve categories of information threats, but we can classify them into three broader categories: the first category of threats includes threats that can be classified as accidental or unintentional, such as force majeure. nature or natural disasters; the second category of threats includes intentional or deliberate threats such as malware attacks, piracy, piracy, denial of service (DoS) attacks, unauthorized access, etc. [1-2].

2. Material and Method

2.1. The context of Albania as a country towards technological development

An important aspect is the context of the place where the phenomenon is being studied. Albania is a developing country with a high middle income, but the terminology "developing country" does not mean that all developing countries experience the same development. Each country has unique political and economic constraints. Ultimately, these restrictions will impose various issues related to security management information. It is important to note that Albania has experienced rapid development in terms of information and communication technology (ICT) in the last decade. During this time the number of internet users has increased spectacularly. The purpose of this paper is to analyze information security practices in Albanian public and private health care institutions, in order to determine which is the level of Information Security in public institutions and to provide suggestions for improvements. Due to the nature of the problem, as a research method we will use the qualitative descriptive research method, while as a technique for data collection we will use questionnaires which are mainly qualitative. Data analysis is mainly based on exploratory data analysis. This paper will use the method of qualitative descriptive research because as he says, qualitative descriptive study is the method of choice when a direct description of the phenomenon is desired. Descriptive research aims to shed light on current issues or problems through a data collection process that enables them to describe the situation more fully than would be possible without using this method. Three main purposes of descriptive studies can be explained as describing, explaining and validating research findings. Descriptive studies are closely related to observational studies, but they are not limited to the method of data collection from observation. Case studies and questionnaires can also be specified as popular data collection methods used with descriptive studies. In our study we used questionnaires as the primary source of data collection. As part of the selected methodology, we also considered the documents of the institutions included in this study [3].

2.2. Objectives of the paper

The purpose of this paper is to analyze the security of information in the health system, for:

- Identify, define and discuss information security management practices and what are the factors that can influence the implementation and development of information security management in Albanian public institutions.
- Understand the importance of the components identified and how they interact with each other.
- Determine the level of information security awareness in public institutions and determine whether improvements can be made in information security management.

In order to achieve the objectives of this study, we have considered the following research questions.

1. What are the security management practices of information in the health system?

The literature on information security management emphasizes the need to address technical and non-technical issues related to information security. Especially in developing countries there is a lack of attention in

the literature to address these issues as well as the level of awareness on information security. Appropriate measures must therefore be taken to protect the critical assets of the health organization.

2. What are the factors that influence the effectiveness of information security management practices?

This question seeks to identify and understand the factors associated with information security management by doing a literature review in general and for the health system in particular focusing on developing countries.

3. How can information security be improved in the Albanian health system?

This question seeks to lay out concrete steps that need to be taken to improve information security in the Albanian health system based not only on the literature, but also on the common characteristics that these institutions have.

Other factors that give importance to this study are:

1- Lack of studies on information security in Albania.
2- Relatively new developments in terms of information security in the health care system in our country.

As limitations of this study, we can mention the lack of academic studies in the field of safety in the health system in Albania. The questionnaire design phase took longer than anticipated as there were difficulties in completing the questionnaire in its initial version in the pilot phase. The data collection phase of the study also took longer than anticipated due to the difficulty in obtaining the response of the respondents. Reasons may include lack of familiarity with the questionnaires, low culture of collaboration in such studies, lack of information and misunderstanding of the purpose of this study [4].

All three research questions focus on the current state of information security in the health system, interactions and processes.

2.3. Risk identification

A very sensitive sector is also the part of surveillance equipment such as oxygenation equipment (case of covid-19), "clothes" equipment which are assisted by the elderly or blind, etc.

Also, another very important and sensitive aspect is the hospital database. These are very sensitive patient data that would directly affect privacy. Another aspect is the management system used by health centers and hospitals in Albania.

What are the risks when it is known that any visit or examination should be scheduled in the system. As a result, traces of this visit remain in the system and his privacy can be compromised, but can be interfered with by changing dates, causing damage to people's lives.

The first step in identifying risks is to identify all elements, assets and resources that belong to the computer system and may be at risk the system classifications are as follows:

- Hardware, e.g., central server, magnetic disks, shredders.
- Software, e.g., operating systems, application programs, backup copies; • Data and media, e.g., program documentation, documentation of operating procedures.
- Communications, e.g., internet lines, telephone lines, computer networks, etc.; • The environment, e.g., electrical network, plumbing, air conditioning; cleaning services.
- Organized, e.g., regulations and management policy.
- Supports, e.g., maintenance staff.
- The preparation of these lists including all endangered elements should be considered in relation to the types of risks and the causes of these risks**.** Risks can be classified:
- Loss of property, e.g., destruction, damage, loss, theft, pollution; • Loss of responsibility, e.g., breach of contract, breach of copyright, defamation, insult.
- Loss of staff, e.g., death, injury, illness, resignation, labor conflict; • Financial losses, e.g., bad debts, dishonest employees.
- Loss of business interruption, e.g., delayed money movements, increase in labor costs, penalties clause.

2.4. Data analysis

In this study, questionnaires were used to collect the desired data in the health system in Albania. The "Respondent Data Questionnaire" was used in data collection by medical students. The selected questions were taken from questionnaires based on international standards on information security, which were used to study information security in the health system in developing countries. In the questionnaire "The questionnaire was

used to collect data from pharmacy students in the faculty of medicine, respectively questions which are related to information security in the health system. Data analysis is necessary to understand the data collected and use it efficiently. The analysis of the data obtained from the survey will help us to have a clearer picture on the security of information in the health care system and what students think. In this research the collected data are categorized and coded to be further processed with the statistical program SPSS (Statistical Package for Social Studies). SPSS enables data to be encrypted and stored in a flexible and effective manner, and provides tools for classifying, sorting, and arranging information. In this section we have explained the processes and procedures that have been used to collect and analyze the data in this study, to achieve the research objectives. Through this research we aim to analyze and understand the security of information in Albanian public institutions by surveying medical students. The qualitative descriptive research method has been selected to achieve the research objectives, using questionnaires as a way to better understand the problem and find appropriate solutions. Above is presented the analysis of data collected through questionnaires [5].

2.5. Some of the survey questions

Do you trust the current system in place in terms of personal data security?

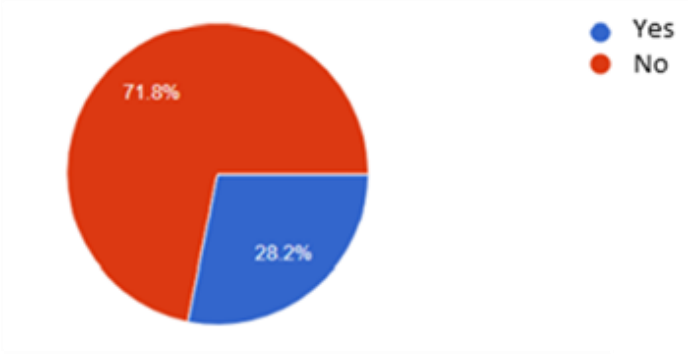

Figure 1. Levels of trust in personal data security systems.

Are you afraid that your data will become more vulnerable if healthcare were digitized?

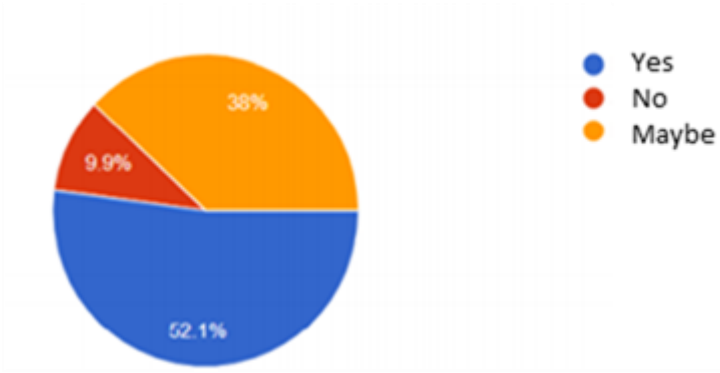

Figure 2. Concerns about data vulnerability in healthcare digitization.

Do you know the terms cybernetics, cyber-security, Information System Security?

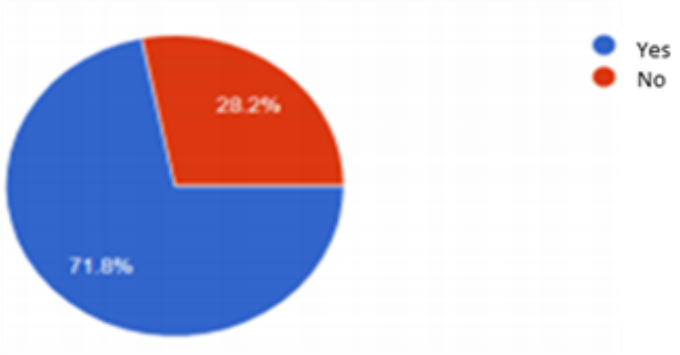

Figure 3. Awareness of key information security terms.

Are you aware of how the health care system works in polyclinics?

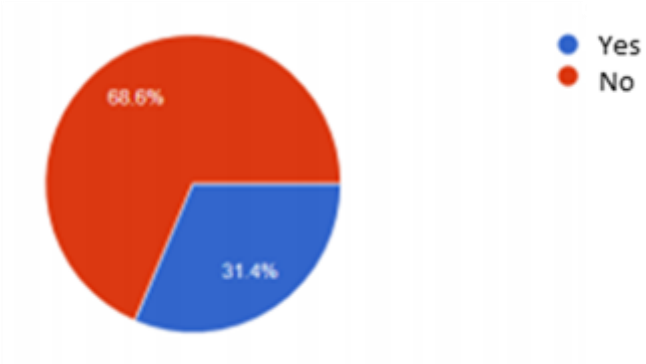

Figure 4. Understanding of polyclinic healthcare system.

Do you have information on where your medical records are stored in these health centers?

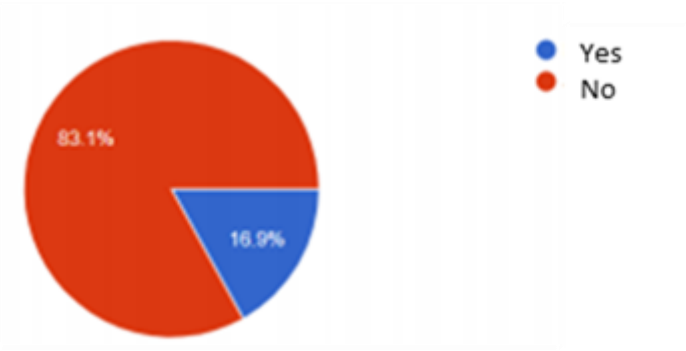

Figure 5. Awareness of medical records storage in health centers.

3. Results

Regarding concerns about the security of personal data in a digitized healthcare system, 52.1% of respondents expressed a high level of fear that their data would become more vulnerable (Figure 2). This indicates that a significant percentage of respondents are worried about the security of their health data. A smaller percentage, 9.2%, stated that they have no fear, while 38% of respondents answered "Maybe," indicating a certain degree of uncertainty or ambiguity on this issue. Interesting is the fact that they understood the importance of information security and had doubts whether this information was being used by others. Most of them were pursuing higher education or had completed them.

Regarding respondents' familiarity with terminology in the field of information security, 71.8% of them claimed to have knowledge of these terms (Figure 3). This shows that a large majority of respondents are informed about concepts related to information security and related aspects. On the other hand, 28.2% of respondents are not familiar with these terms, indicating that there is a certain percentage of respondents who are not acquainted with information security terminology.

Through the analysis of these results, it can be observed that data security in a digitized healthcare system is an important issue for respondents, and there is a varying degree of familiarity with terms related to information security (Figure 4). This information can be used to shape policies and strategies to address data security concerns and to increase awareness about information security in these specific contexts.

Most of the respondents indicated that there are still problems and uncertainties in the health system about information security. However, regarding the management of information security in the country by hospitals, 71.8% answered that they do not trust the information system in the country (Figure 1), it is also noted that respondents do not have information about digitalization of health. 38% answered that I am not sure if digitalization would bring information insecurity and make it even more easily accessible by illegal organizations or structured groups of hackers dealing with information theft (Figure 2).

Also, 46.5% of respondents do not read private matters at all when they become part of the health system in the country [6-7].

When asked about their awareness of the location where their medical records are stored in health centers, a significant majority of respondents, specifically 83.1%, answered "no." (Figure 5). This suggests that a large

portion of respondents is not aware of the precise location where their medical records are kept within health centers. Conversely, a smaller percentage, 16.9%, responded with "yes," indicating that a minority of respondents do have knowledge of the storage location of their medical records in these healthcare facilities (Figure 5).

These findings highlight that a substantial number of individuals lack awareness regarding the specific storage of their medical records within health centers, which could have implications for data access and security awareness in healthcare settings.

4. Discussion

The literature on information security management emphasizes the need to address technical and non-technical issues related to information security. Especially in developing countries there is a lack of attention in the literature to address these issues as well as the level of awareness on information security. Appropriate measures must therefore be taken to protect the critical assets of the health organization. This question seeks to identify and understand the factors associated with information security management by doing a literature review in general and for the health system in particular focusing on developing countries [8].

5. Conclusion

From the analysis of the questionnaires for the analysis of trust in the health system as well as the security of information in Albania, we identified that:

- The largest percentage of respondents are women with 81.4%, this large percentage of women as the field where we are focused to do this study is mostly chosen by women, the respondents are medical students in the field of pharmacy.
- The 19-25 age group is 90% of the respondents, this was known in advance as the respondents are students. This age group was chosen to be surveyed as they are more inclined in the field of information technology and have more knowledge about digital medicine.
- Respondents were also asked about their education and almost 70% of them had a bachelor's degree, most of them were still studying. A very small part of them were employed.
- A considerable part of them did not understand the term cybernetics even though they are the age group of technology, they had problems in filling out the forms and little known for this category even though they are students in the field of pharmacy. This further complicates healthcare digitalization as pharmacists should be the first to use this system to see prescriptions issued by doctors in a future where healthcare will be digitized. This brings many obstacles on the way to a total digitalization of it.
- Only a small number of them knew how polyclinics worked, and a large number of them had no idea how to book a place for a polyclinic analysis from polyclinics in the country. A large proportion of about 62% of respondents have never had a check-up at a polyclinic. 21% who had had this type of control had a pronounced lack of confidence that their analysis would be safe in health systems.
- Nearly 83% of them were not aware of where the card analysis data or medical prescriptions were stored, they are not fully informed. Polyclinics in the country have never asked permission to use the data of their clients, this is noted in the survey we conducted where 83% of them say that this type of request has never been made, except in cases where polyclinics have asked to do any specific statistics. But there are also many cases where the data is used without the consent of the person who owns this data.
- Again, there is a marked lack of information regarding data security where it is clear that there are uncertainties in data breach, i.e., whether this data can be accessed and used by others. Most of them wanted their medical records to never be made public and lacked confidence in this part. The bulk followed by 87% was the medical card with all the details and then personal name, nationality, address and personal information were another detail that the respondents would like to be very safe in the health system in the country.
- Privacy policies were another detail in this study where it was clearly noted that a majority of 46% did not read them before agreeing to them. This can sometimes have a detrimental effect as in a private polyclinic if you approve these terms, it may use the data for marketing reasons or other actions specified in the private matter you have previously received. Most respondents state that they have never given permission to third parties to use their data only in cases where they have not read it at all.
- Respondents think that digitalization of health will affect information security and make it more vulnerable to certain organizations, others surveyed have no idea if this will make any difference in information security. Again, a marked lack of information.
- Lack of trust in health has been discussed for years in our country, even today this wound remains open as well as in the security of information stored in these institutions. Medical students do not trust the current information management system in the health system in the country. They think that this information stored there is prone to be accessed by unauthorized individuals at any time.

- From the conclusions obtained from the analysis made in our study, we have identified the improvements that need to be made for a successful management of information security in the health system.
- For a better implementation of the security strategy and policies it is necessary to select and implement information security standards. Due to the similarities that the health system has with each other, it is recommended to select and implement the same standard for information security and respectively the ISO standard, which is one of the most well-known international standards. Its implementation in all hospitals will provide the necessary experience for their application.
- It is also important to do risk assessment for all public hospitals, and they can benefit greatly from this process. Without a risk assessment process, hospitals will never be sure that they have chosen the right strategy for protecting the institution's information.
- Awareness of information security needs to be raised. Health institutions should support education and training programs for information security for all health system employees who deal with digital devices connected to the network. These trainings should be done frequently, to always bring to attention the importance of information security.
- With the Decision of the Council of Ministers no. 673, dated 22.11.2017, "On the reorganization of the National Agency of Information Society", it was decided that within the NAIS, at each institution and state administration body under the responsibility of the Council of Ministers to establish and operate Technology units of Information and Communication. So, for all institutions, ICT units will depend on NAIS. For a successful implementation of information security, it is necessary to create or assign personnel responsible for information security, who should be at the management level. To make a better balance of these positions I would recommend that the personnel responsible for information security depend on AKCESK, the agency responsible for cyber security.
- Although, as we have mentioned above, the GDPR, in our country will be implemented by Albanian companies that have relations with the European market, in the priorities of the Commissioner for the Right to Information and Personal Data Protection for 2018 is defined… " Approximation of legislation on personal data protection with EU Regulation 679/2016 and Directive 680/2016" (Commissioner for the Right to Information and Personal Data Protection, 2018). To be proactive in terms of personal data protection and privacy, I recommend that the Albanian public and private health systems (hospitals) take into account the GDPR, in the construction or improvement of ICT systems [9-10].

Acknowledgement

This study was partly presented at the 6th Advanced Engineering Days [10].

Funding

This research received no external funding.

Author contributions

Dolantina Hyka: Conceptualization, Methodology, Writing-Original draft preparation, analyzing the survey
Fatmir Basholli: Data curation, Writing-Reviewing and Editing

Conflicts of interest

The authors declare no conflicts of interest.

References

1. Hyka, D., Hyra, A., Basholli, F., Mema, B., & Basholli, A. (2023). Data security in public and private administration: Challenges, trends, and effective protection in the era of digitalization. Advanced Engineering Days (AED), 7, 125-127.
2. Basholli, F. (2022). Cyber warfare, a new aspect of modern warfare. VI International Scientific Conference: Theoretical foundations of security national and international security information security technical facilities for ensuring security, 05-08. December 2022 Borovbets, Bulgaria, 52-54
3. Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1-10. https://doi.org/10.3233/THC-161263

4. Alharam, A. K., & Elmedany, W. (2017, May). The effects of cyber-security on healthcare industry. In 2017 9th IEEE-GCC Conference and Exhibition (GCCCE) (pp. 1-9). IEEE. https://doi.org/10.1109/IEEEGCC.2017.8448206
5. 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
6. Ahmad, A. (2012). Type of security threats and it's prevention. International Journal of Computer Technology and Applications, 3(2), 750-752.
7. Basholli, F., Daberdinİ, A., & Basholli, A. (2023). Detection and prevention of intrusions into computer systems. Advanced Engineering Days (AED), 6, 138-141.
8. Hyka, D., Premti, F., & Boce, G. (2019). Creating strong and diagnostic systems. The case of elgamal digital signature over ECC. Inovation, mathematics and information technology, 1, 194-198
9. Daberdini, A., Basholli, F., Metaj, N., & Skenderaj, E. (2022). Cyber security in mail with Fortiweb and Fortinet for companies and institutions. Advanced Engineering Days (AED), 5, 81-83.
10. Hyka, D., & Basholli, F. (2023). Health care cyber security: Albania case study. Advanced Engineering Days (AED), 6, 121-123.

© Author(s) 2023. This work is distributed under https://creativecommons.org/licenses/by-sa/4.0/