Security Systems in Greek Health Care Institutions: a Scoping Review Towards an Effective Benchmarking Approach

Savina Mariettou, Constantinos Koutsojannis and
Vassilios Triantafillou

December 4, 2023

Security systems in Greek health care institutions: A scoping Review towards an effective benchmarking approach

Savina Mariettou*, Constantinos Koutsojannis**, Vassilios Triantafillou***

**University of Peloponnese, Electrical and Computer Engineering Department, Patras, Greece*

***Professor of Medical Physics & Electrophysiology, Director of Health Physics & Computational Intelligence Laboratory, Physiotherapy Department, School of Health Rehabilitation Sciences, University of Patras, Patras, Greece.*

****Professor of Network Technologies and Digital Transformation lab, Electrical and Computer Engineering Dpt., University of Peloponnese. Patras, Greece*

ABSTRACT

Healthcare has undoubtedly brought many advancements through information technology. Specifically, healthcare informatics involves the use of various technologies, data management and communication systems to collect, store, analyze and effectively disseminate information. Therefore, the above serves to improve care as well as patient outcomes, improve efficiency, promote innovation and data analysis, as digitization has become an integral part of our daily lives in today's world. However, with the increased use of interconnected systems and electronic health records, hospitals have become prime targets for cyberattacks. In this article we will delve into the critical topic of cybersecurity in hospitals as well as nursing facilities. The deepening of this issue was carried out with extensive analysis of the security systems of Greek hospitals. We investigated all their web sites and the security systems already in place on those sites. By checking we found a number vulnerabilities and potential risks. The most important weakness is the lack of legal as well as technical information for all interested citizens and patients. More organizational as well as technical work concerning internal architecture of information systems is needed, towards the improvement of security. In conclusion, we present our proposals on strategies to strengthen healthcare facilities against cyber threats.

KEYWORDS

Healthcare, information, systems, patients, digitization, cybersecurity.

1. INTRODUCTION

In this article we present an extensive analysis of the security systems of the hospitals of Greece. The main objective of first section is to explain how security became increasingly important, providing a chronological review of the evolution of health information technology including the developing stages of health systems.

1.1 Historical review of computer system in healthcare

Starting in 1960, experts on information systems realized that protecting the organization was not limited to fire hazards and criminal activities (York and MacAlister, 2015). In the 1960s, computers evolved in two stages. At the beginning of mini-computers and along the way they evolved into microcomputers (Berner, Detmer and Simborg, 2005). The late 1960s saw an important period in the development of information systems in hospitals. Some systems integrate patient diagnoses, patient information, and care plans based on physician and nurse orders. This development represents a remarkable step forward in the digitization of healthcare information and the potential for more comprehensive patient care management (Saba, Johnson and Simpson, 1994). In general in the 1960s and 1970s, it was perceived in all departments and functions of the health organization as a time of rebirth (York and MacAlister, 2015). The use of informatics in health care began with the first applications mainly for administrative and fiscal functions in hospital settings. However, there were still hesitations about the use of these systems by experts, as evidenced by the increasing number of pharmaceuticals and the increase in laboratory tests and diagnostic equipment (Berner, Detmer and Simborg, 2005). In the 1970s, object- oriented databases started being used (Gharote et al., 2022). It is worth noting that after our research we found that cyber-attacks, also known as threats or attacks, appeared in the late 1970s. These attacks were widespread in various sectors, including medical care. What initially manifested as spam eventually evolved into more malicious forms such as viruses and malware (Cs et al., 2017). The 1980s was an important era in health informatics (Ambinder, 2005). The volume and complexity of patient data as well as health records increased significantly (Gharote et al., 2022). For the first time in 1983, Microsoft Windows appeared. The methodologies and systems of this period were intended to support clinical decision making in healthcare and focused on clinical diagnosis providing optimal patient care. At the same time, health level 7 (HL7) highlighted the importance of electronic data exchange in healthcare. This has an impact on improved interoperability and information sharing between different healthcare systems. Clearly, the method improved the quality of patient care. However, despite the increased potential, the development of health information systems has faced challenges. Hospitalization-related diagnostic groups and the need for managed care have increased pressure on health care to control costs. This means that, despite the need to integrate information systems in hospitals, the budget was quite limited for the development and maintenance of these systems. As a result, the implementation of health information systems in the 1980s faced funding challenges, despite predictions of improving patient care and reducing costs (Ambinder, 2005). In the 1990s, the rise of healthcare systems was significant (Ambinder, 2005). Health Management Information System has begun to be adopted by more and more countries in the hospital environment (Gharote et al., 2022). The sheer volume of this data allowed users to access this information without controls, and the main issue was how it allowed them to use it. Patient privacy soon emerged as an obstacle. This concern culminated with the passage of (HIPAA) (Ambinder, 2005). HIPAA appeared in 1996, known as the federal law enacted to protect sensitive health information. HIPAA mandatory physical safeguards include the use and security of workstations, device and media controls, and facility access controls (Cs et al., 2017). In the early 2000s, the synergies between Information and Communication Technologies and medical and healthcare practices rapidly converged and enabled a key cornerstone in this field: electronic healthcare (e-health). This development was significant and enabled, among other things, the provision of medical services via the Internet, the management of electronic records by standards and the communication between patients and health professionals. At the same time, it is worth noting that mobile healthcare (m-health) also appeared for patient care. Taken together, they marked a significant shift towards *digitization in healthcare*, which brought greater security challenges and increased awareness of the need to protect patient information. Healthcare organizations have invested in security measures, policies and technologies to protect sensitive personal health data (Batista et al., 2021).

In the 2010s, a defining moment was on 2015. The World Health Organization report on countries and health care organizations around the world noted the priority of information systems in health care (Fernandes et al., 2022). Also, in the first decade of the 21st century, COVID-19 posed a challenge to the global healthcare system (He et al., 2020). From the beginning of the second decade of the 21st century until today, Hospital Management Information Systems have evolved a lot. The main role is to improve healthcare service delivery, patient care and administrative efficiency. Information systems have become a key tool for modern healthcare institutions, supporting them in delivering high-quality care, optimizing operations and adapting to the evolving healthcare landscape. In addition to the above, information systems offer a wide range of software and services integrated into the facilities that a hospital has in order to serve them as best as possible. These information systems range from large hospitals to smaller clinics and nursing homes. Over the years, healthcare delivery, data management (Gharote et al., 2022) and obviously the security of these systems is expected to improve further. Therefore, in general, we can analyze the stages of development of the health system. The time distribution could be recorded as follows.

- ***Healthcare 1.0 (18th - early 20th century)***: At this stage, the technology was limited but used for basic medical applications such as anesthesia and precision in blood measurements.
- ***Healthcare 2.0 (1920 - 2010)***: This stage was accompanied by the development of the Internet, as well as the industrialization of health care. Internet health applications and online appointments are important.
- ***Healthcare 3.0 (1990 - 2020)***: The third stage focused on the development of the World Wide Web and the interconnection of electronic health data. An increase was also observed in the use of electronic health services.

- ***Healthcare 4.0 (2015 - present)***: During the present phase, artificial intelligence and intelligence have been introduced into medical services. This has led to advanced applications such as autonomous diagnosis and personalized therapy. The goal of improving the quality of care, expanding access to healthcare and enhancing health intelligence are part of this development. Healthcare 4.0 continues to evolve, supporting high-quality care and a customized approach for each patient (Ahmad et al., 2022).

1.1.1 Challenges

Reviewing the bibliography and the effort to improve the quality of care, some challenges have been created. The challenges of data security, privacy and trust building are indeed significant in today's cyber-threat-dominated world (Gharote et al., 2022). We identified research which focused clearly on the challenges and solutions in the health sector. At the figure 1 there will be a brief review so that we understand the importance of security in healthcare (He et al., 2020).

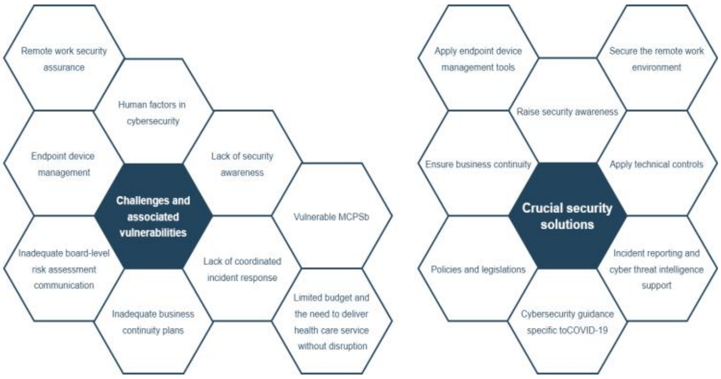
Remote work security assurance
Human factors in cybersecurity
Endpoint device management
Lack of security awareness
Challenges and associated vulnerabilities
Vulnerable MCPSb
Inadequate board-level risk assessment communication
Lack of coordinated incident response
Inadequate business continuity plans
Limited budget and the need to deliver health care service without disruption
Apply endpoint device management tools
Secure the remote work environment
Raise security awareness
Ensure business continuity
Apply technical controls
Crucial security solutions
Policies and legislations
Incident reporting and cyber threat intelligence support
Cybersecurity guidance specific toCOVID-19

Figure 2: Challenges and solutions in the health sector

2. SECURITY

Based on what we have analyzed above, "*Healthcare 4.0*" specifically addresses the ways in which the 4th Industrial Revolution is reshaping the healthcare industry. But attention should be directed to the security of the systems. Specifically, the qualities CIA trinity (Confidentiality, Integrity and Availability) serve as the basis for designing comprehensive security policies, practices and controls in an organization. The main threats are cyber-attacks, data breach and unauthorized access. For example, there are data protection laws such as GDPR or HIPAA specifically in the health sector. These laws take basic considerations for compliance dealing with (Sarker, 2021):

- ***Confidentiality***: The aspect is concerned with keeping sensitive information confidential and protecting it from unauthorized access. It ensures that only people or systems with appropriate rights can access certain data. Examples include the protection of patient health records in healthcare institutions and intellectual property in research organizations (Al-Issa, Ottom and Tamrawi, 2019).
- ***Integrity***: Maintaining data integrity means ensuring that information remains accurate and reliable. In health care, this violation could lead to incorrect treatment (Gritzalis and Lambrinoudakis, 2004).
- ***Availability***: Availability focuses on ensuring that systems and data are accessible when needed by authorized users. In healthcare, availability is critical because patient data and systems must be accessible 24 hours a day (Computer security for data collection technologies, 2018).

2.1 Cybersecurity and Related Terms

"*Cybersecurity*" and related terms that have separate meanings in practice are very interconnected. Let's clarify these terms:

- ***Information Security***: focuses specifically on the protection of privacy, integrity and availability of information. This security can be divided into digital or physical forms. This term has under its umbrella data security, information systems and risk management related to information management (Sarker, 2021).
- ***Data Security***: is related to information security as we said in the above term. Its main objectives are the protection of data from unauthorized access or illegal use. It includes encryption, access controls, and other measures to protect data at rest, in transit, and during processing (Al-Issa, Ottom and Tamrawi, 2019).
- ***Network Security***: focuses on the security of communication channels. In network protection, we will often see security measures such as firewalls, intrusion detection systems and VPNs.
- ***Internet/IoT Security***: refers to the security of activities and transactions conducted over the Internet (Sarker, 2021). Adapting this term to the context of the health sector results in the Internet of Medical Things (IoMT). IoMT refers to the network of medical devices and applications that are interconnected over the Internet and collect and exchange data to improve patient care, improve operational efficiency, and advance medical research (Lee, 2023).

2.1.1 Types of Cyber Security Systems

According to publications in the HIPAA magazine, how information systems should provide the required security and taking the necessary awareness from what is mentioned, we deepen the types of security of information systems in cyberspace from any kind of cyber-attack (HIPAA Journal, 2018). Therefore by studying identify the following.

1. Firewalls are key network security devices that monitor and filter incoming and outgoing network traffic (Gharote et al., 2022).

2. The intrusion detection system (IDS), defined as a device or software application. Monitors network traffic and systems for any suspicious activity or fraud. It collects data from various sources and thus is able to detect breaches as well as internal and external attacks (Sarker, 2021).

3. Intrusion Prevention Systems (IPS) that receives a threat and the intrusion prevention system (IPS) can be used to avoid and block it. This is achieved in a number of ways, including manual sending, notification sending or automation (Sarker, 2021).

4. Antivirus. Anti-malware software is defined as antivirus software. Its use is to detect and remove computer viruses or malware or even prevention (Sarker, 2021).

5. Email Security Systems as is a primary means of communication in healthcare organizations. Because large amounts of information are stored, email security solutions protect against phishing attacks, spam and email-borne malware, which are common attack vectors.

6. Security Checks, specifically divided into two categories *basic* and *advanced* security controls. Key controls include virus protection, file/data backup and restore, data loss prevention, email gateway, encryption, incident response plan, detection and system intrusion prevention, mobile device management, secure deployment, security awareness training, vulnerability management and web portal. Advanced security controls include anti-theft devices, digital forensics, multi-factor authentication, network segmentation, penetration testing, threat intelligence sharing, vulnerability scans (HIMSS, 2020).

3. METHODOLOGY

In order to gather the relevant information for my review article, I conducted a comprehensive search from 1 May 2023 to 15 November 2023. This search involved investigating a wide range of reliable sources, databases and academic journals to ensure that the information included is timely, reliable and comprehensive. Therefore, the databases used include Google Scholar, Science Direct, IEEE and Hospital Websites.

Finally in this paper we have investigated 126 (47% of total in Greece) or 100% of publicly owned hospitals in Greece according to (Statista, 2023) and representing all Greek Health Regions according to ministry of health division.

4. SECURITY IN GREEK HOSPITALS

The components of risk management are variable. It can be safety, environmental safety, worker health, worker safety, patient safety, medical audits, disaster program, infection control, insurance/claims management, product evaluation, evaluation of contracts, incident reporting/review/action, Biomedical Instrument Testing (York and MacAlister, 2015). Before starting our analysis of all hospitals by region, we identified a survey published in 2009. It is based on the integration of IT and communication technologies in all public hospitals in Greece. Specifically, in 132 hospitals, 77% of hospitals have an IT department, while only 52.7% have an Integrated Information System. Finally, the 5th and 6th Health Regional show the greatest shortage in IT departments, since 5 of the 12 hospitals of the 5th (41.7%) and half (11 out of 22) of the 6th (50%), do not have an IT department. On the other hand, the best pictures are presented in the 3rd (93.8%), the 4th (92.9%) and the 1st Health Regional (91.7%) (Stamouli et al., 2009). Based on these, we did research by checking all the websites of the hospitals in Greece, observing what information is written about the security of the information systems in each hospital.

Hospital Name	Policy Name	Description	Reference
«Evangelismos», «Panagiotis & Aglaia Kyriakou», «Sismanoglio», «Amalia Fleming»	firewalls	security measure that restricts access to the network and protects against unwanted access attempts	(1st YPE, 2023)
«Evangelismos», «Panagiotis & Aglaia Kyriakou», «Children's Penteli Hospital»	intrusion detection and prevention (IDS/IPS)	systems that detect and prevent network intrusions	(1st YPE, 2023)
«Evangelismos», «Panagiotis & Aglaia Kyriakou», «Sismanoglio», «Amalia Fleming», «Sotiria»	cryptography	protect data confidentiality	(1st YPE, 2023)
«Evangelismos», «Agia Eleni - Spiliopouleio», «Agia Sophia Children's Hospital», «Agios Savvas», «Konstantopouleio», »Alexandra», «Hippokrateio», «Pammakaristos», «Gennimatas», «Laiko», «Elena Venizelou», «KAT», «EKA», «Sotiria», «Thessaloniki - Agios Pavlos», «Halkidiki», «Kilkis», «Serres», «Kavala», «Didymoteicho», «Alexandroupolis», «Komotini», «EKA», «Veria», «Edessa», «Kastoria», «Florina», «Bodosakeio», «Giannitsa», «Naousa», «Thebes», «Chalkida», «Kimi», «Karystos», «Karpenissi», «Amfissa», «Lamia», "Kalymnos - Vouvaleio», «Karpathos», «Thira», «Nikaia Piraeus - Agios Panteleimon» , «Syros - Vardakeio and Proio», «Leros - State Sanatorium », «Kos - Hippokrateion», «Chios - Skylitseio», «Samos - Agios Panteleimon», «Mytilene - Vostaneio», «Lemnos», «Ikaria», «Metaxa», «Psychiatric» , «Elefsina - Thriasio», «Dromokaitio», «Argos», «Tripoli», «Ioannina - Chatzikosta», «Preveza», «University Hospital - Ioannina», «Molos», «Amaliada», «University Hospital - Patras», «Rethymno», «University Hospital of Heraklion», «Health Center of Sitia»	personal data, privacy policy	passwords, personal data (GDPR), cookies	(1st YPE, 2023), (2nd YPE, 2023), (3rd YPE.gr, 2023), (4YPE, 2021), (Dypethessaly.gr, 2020), (6th YPE, 2021), (7th YPE Crete, 2012)
«Korgialeneio-Benakeio», «Sismanoglio», «Amalia Fleming», «Sotiria»	infrastructure and communications	protection of information systems,	(1st YPE, 2023)

	management	communications and infrastructure management	
«Papanikolaou», «Gennimatas–Agios Dimitrios», «KAT», «Veria», «Edessa», «Mamatsio», «Florina», «Grevena», «Giannitsa», «Papageorgiou», «Thessaloniki - Agios Pavlos», «Serres», «Kavala», «Xanthi», ««University Hospital - Larissa», «Volos», «Trikala», «Karpenissi», «Amfissa», «Lamia», «Argos»,«Nafplio», «Kalamata», «Kyparissia», «Corinth», «Tripoli», «Zakynthos», «Corfu», «Kefalonia», «Lefkada», «Arta», «Ioannina - Chatzikosta», «Preveza», «University Hospital - Ioannina», «Molos», «Agrinio», «Mesolongi - Chatzi-Kosta», «Aigio», «Kalavryta», «Pyrgos», «Amaliada», «Krestena», «Patras - Agios Andreas», «University Hospital - Patras», «Karamandan», «Heraklion - Venizeleio-Pananeio», «Agios Nikolaos»		integrated information system (organization responsibilities)	(3rd YPE, 2023), (4YPE, 2021), (Dypethessaly.gr, 2020), (6th YPE, 2021), (7th YPE Crete, 2012)
«Evangelismos», «Laiko», «KAT», «Gennimatas», «Sismanoglio», «Amalia Fleming», «Agios Savvas», «Panagiotis & Aglaia Kyriakou», «Children's Penteli Hospital», «Agioi Anargyroi», «Agia Sophia Children's Hospital», «Bodosakeio», «Karpathos», «Naxos», «Samos - Agios Panteleimon», Attikon, «Patras - Agios Andreas», «University Hospital - Patras», «University Hospital - Ioannina», «Health Center of Sitia»		integrated information system	(1st YPE, 2023), (2nd YPE, 2023), (3rd YPE, 2023), (6th YPE, 2021), (7th YPE Crete, 2012), (Uhi.gr, 2023)

Table 1: Analysis of Greek Hospital websites: posted information for patients/ citizens

Security systems data were collected in details (Table 1). We recorded the main website which shows all hospital websites by Health Regional separately. In particular, in the first Health Regional there are a total of 24 hospitals. In the time frame we worked the «Polyclinic» and «Agioi Anargyri» General Oncology Hospital of Kifissia city, did not have a website available. Even in the «Ophthalmology Hospital» there was no mention of anything related to security and privacy. The rest of the hospitals are ranked as follows four hospitals that report that there are "firewalls", hospitals with (IDS/IPS), 5 hospitals with cryptographic tools, and fourteen that refer to privacy policy. Five that note the protection of information, communications and infrastructure management systems. Another 11 hospitals report that they have a complete information system but in a different source, an article as it was not found to highlight anything on the websites. In the second Health Regional we have a total of 24 general hospitals. The General Hospital of Rhodes Island «Andreas Papandreou» website was not available. At the General Hospital - Health Center of Kythira Island «Trifillio» and General Hospital «Asklepieio Voulas», no relevant information was found on their websites regarding the legal framework or security systems. Also, we have 6 hospitals that refer to patient protection and 4 hospitals that state that they have an integrated information system. In the third and fourth Health Regions we have a total of 16 hospitals and 14 hospitals, respectively. In these two Health Regional there does not seem to be any website running through any issues. Specifically, we have eight in each Health Regions that seem to touch on the issue of privacy policy, respectively. 10 hospitals in the third and four hospitals in the fourth reporting information system responsibilities. In the third in 1 hospital, it states that they have a complete information system. It should be noted that the specific hospital also mentions data protection. Finally in the fourth a single hospital integrated information system. In the fifth Health Regional we have a total of 13 hospitals. At the General Hospital of Livadia town website was not available. We found data protection issues recorded in seven hospitals, only one hospital integrated information system and six hospitals with information system responsibilities. In the sixth Health Regional we have a total of 27 hospitals. At the General Hospital of Krestena town and the General Hospital of Lefkada Island, websites was not available. In this region, in addition to the websites, a check was also made on the corresponding legislations since you indicate these on the Health Regional home page. Specifically, we have eight hospitals that refer to privacy policy, 26 hospitals that state the responsibilities of the information system and three hospitals that state that they have an integrated information system. In the seventh Health Regional, we have a total of 8 hospitals. At the General Hospital - Health Center of Neapolis town, no relevant information was found on their websites regarding the legal framework or security systems. At the General Hospital - Health Center of Ierapetra town, website was not available. All the hospitals that were General Hospitals of Greece were not written the term "General Hospital", just the name was used. On these websites, we found that 3 hospitals recorded issues of privacy policy. A single hospital integrated information system and two hospitals with information system responsibilities. According to our results, the security systems, in the posted information that exists, differ from one facility to another. In addition, you do not record to a degree visible to citizens and patients the protection of personal data and the privacy policy. Furthermore, I should note that they themselves do not know to what extent these information systems are secure, to what extent data and information could be exposed and for what reason.

5. CONCLUSION

Hospital and healthcare facility security systems play a critical role in protecting patients. Through our research we have identified several vulnerabilities in these security systems as several hospitals in Greece there is no complete picture of whether there is an information system or the responsibilities of this department that proves its existence. The most important, the citizen has no knowledge about protection and rights. In particular, he does not know how protected he is and how much he could be exposed if sensitive information is leaked. Even with regard to the General Data Protection Regulation, it is not clear who the Data Protection Officer is and how his data is used. The information posted to the citizen or patient is minimal and not clear. Therefore, between security and accessibility, it is necessary to find the right balance without forgetting cost management. In the future, for proper communication and data exchange between these systems, the creation of an effective interface should be tested. Also, we could focus on an architecture that would rely on blockchain technology as a security measure. Finally, benchmarking should be applied, aiming to identify best practices and improve performance (Sponsored by ID Experts, 2016). That is, according to the bibliography with an integrated software it will be possible to improve the privacy of protected health information and data security by complying with HIPAA regulations (Wagner et al., 2002).

REFERENCES

Article

Ahmad, K.A.B., Khujamatov, H., Akhmedov, N., Bajuri, M.Y., Ahmad, M.N. and Ahmadian, A. (2022). *Emerging trends and evolutions for smart city healthcare systems*. Sustainable Cities and Society, 80, p.103695. doi:https://doi.org/10.1016/j.scs.2022.103695.

Batista, E., Moncusi, M.A., López-Aguilar, P., Martínez-Ballesté, A. and Solanas, A. (2021). *Sensors for Context-Aware Smart Healthcare: A Security Perspective*. Sensors (Basel, Switzerland), [online] 21(20), p.6886. doi:https://doi.org/10.3390/s21206886.

Computer security for data collection technologies. (2018). *Development Engineering*, [online] 3, pp.1–11. doi:https://doi.org/10.1016/j.deveng.2017.12.002.

Fernandes, C., Claro, N., Monteiro, S., Pires, I.M. and Gouveia, A.J. (2022). *The evolution of IS/IT in health care in last decades*. Procedia Computer Science, [online] 203, pp.707–713. doi:https://doi.org/10.1016/j.procs.2022.07.105.

HIMSS (2020). *Cybersecurity in Healthcare.* [online] www.himss.org. Available at: https://www.himss.org/resources/cybersecurity-healthcare.

Lee, I. (2023). *Analyzing Web Descriptions of Cybersecurity Breaches in the Healthcare Provider Sector: A Content Analytics Research Method*. Computers & Security, p.103185. doi:https://doi.org/10.1016/j.cose.2023.103185.

Saba, V.K., Johnson, J.E. and Simpson, R.L. (1994*). Computers in nursing management*. American Nurses Association Publications, [online] (NP-87 10M), pp.i–x, 1–42. Available at: https://pubmed.ncbi.nlm.nih.gov/8042715/ [Accessed 14 Nov. 2023].

Sarker, I.H. (2021). *AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions*. www.preprints.org. [online] doi:https://doi.org/10.20944/preprints202101.0457.v1.

Book

York, T. W., & MacAlister, D. (2015). *Hospital and Healthcare Security*. In Google Books. Butterworth-Heinemann. https://books.google.gr/books?hl=en&lr=&id=odacBAAAQBAJ&oi=fnd&pg=PP1&#v=onepage&q&f=false

Journal

Ambinder, E.P. (2005). *A History of the Shift Toward Full Computerization of Medicine*. Journal of Oncology Practice, [online] 1(2), pp.54–56. doi:https://doi.org/10.1200/jop.2005.1.2.54.

Al-Issa, Y., Ottom, M.A. and Tamrawi, A. (2019). *eHealth Cloud Security Challenges: A Survey*. Journal of Healthcare Engineering, [online] 2019, pp.1–15. doi:https://doi.org/10.1155/2019/7516035.

Berner, E.S., Detmer, D.E. and Simborg, D. (2005). *Will the Wave Finally Break? A Brief View of the Adoption of Electronic Medical Records in the United States*. Journal of the American Medical Informatics Association : JAMIA, [online] 12(1), pp.3–7. doi:https://doi.org/10.1197/jamia.M1664.

Cs, K., B, F., T, J. and Dk, M. (2017). *Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends*. [online] Technology and health care : official journal of the European Society for Engineering and Medicine. Available at: https://pubmed.ncbi.nlm.nih.gov/27689562/.

Gharote, Y., Jatakia, R. and Nagare, D.G. (2022). *Evolution, Prospects, and Challenges in Hospital Management Information System: Case Studies*. International Journal of Engineering Research & Technology, [online] 11(11). doi:https://doi.org/10.17577/IJERTV11IS110082.

Gritzalis, D. and Lambrinoudakis, C. (2004). *A security architecture for interconnecting health information systems*. International Journal of Medical Informatics, [online] 73(3), p.305. Available at: https://www.academia.edu/19626212/A_security_architecture_for_interconnecting_health_information_systems [Accessed 14 Nov. 2023].

Stamouli, T., Tsikrika, I., Tsikrikas, N., Tsaklakidou, E., Apostolakis, A., & Kyriopoulos, A. (2009). *Informatics in Greek public hospitals: Its use by hospital executives*. Hellenic Statistical Institute, Proceedings of the 22nd Panhellenic Statistical Conference, pp. 191–200.

Statista. (2023). Publicly owned hospitals in Greece 2002-2021. [online] Available at: https://www.statista.com/statistics/557195/publicly-owned-hospitals-in-greece/ [Accessed 17 Nov. 2023].

He, Y., Aliyu, A., Evans, M. and Luo, C. (2020). *Healthcare Cyber Security Challenges and Solutions Under the Climate of COVID19: A Scoping Review (Preprint)*. Journal of Medical Internet Research, [online] 23(4). doi:https://doi.org/10.2196/21747.

Wagner, J.R., Thoman, D.J., Anumalasetty, K., Hardre, P. and Ross-Lazarov, T. (2002). Benchmarking HIPAA compliance. Journal of healthcare information management: JHIM, [online] 16(2), pp.46–50. Available at: https://pubmed.ncbi.nlm.nih.gov/11941920/ [Accessed 17 Nov. 2023].

Report

Sponsored by ID Experts (2016). Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data. Ponemon Institute LLC.

Websites

HIPAA Journal (2018). *HIPAA Compliance Checklist*. [online] HIPAA Journal. Available at: https://www.hipaajournal.com/hipaa-compliance-checklist/.

1st YPE, (2023). *Hospital – 1st Regional Health Authority*. [online] Available at: https://www.1dype.gov.gr/?page_id=70.

2nd YPE, (2023). *Public Hospital* – 2nd D.Regional Health Authority Piraeus & Aegean. [online] Available at: https://www.2dype.gov.gr/dimosia-nosokomeia/.

3rd YPE, (2023). *Hospital*. [online] Available at: https://www.3ype.gr/menutop-foreisygeias/menutop-nosokomeia.

4th YPE, (2021). *Hospital Contact Details | 4th YPE Macedonia & Thrace*. [online] Available at: https://www.4ype.gr/e-s-y/stoicheia-epikoinonias-nosokomeion/.

Dypethessaly.gr. (2020). *5th YPE.* [online] Available at: https://www.dypethessaly.gr/#contactnav.

6th YPE (2021). L*egislation – Organizations Hospitals – 6th Regional Health Authority*. [online] Available at: https://www.dypede.gr/%ce%bd%ce%bf%ce%bc%ce%bf%ce%b8%ce%b5%cf%83%ce%b9%ce%b1-%ce%bf%cf%81%ce%b3%ce%b1%ce%bd%ce%b9%cf%83%ce%bc%ce%bf%ce%b9-%ce%bd%ce%bf%cf%83%ce%bf%ce%ba%ce%bf%ce%bc%ce%b5%ce%b9%cf%89%ce%bd/.

7th YPE Crete. (2012). Www.hc-Crete.gr. Retrieved November 15, 2023, from https://www.hc-crete.gr/MonadesYgeias/home/nosokomeia.

Uhi.gr. (2023). *Yphresia Informatics– University General Hospital Ioannina*. [online] Available at: https://uhi.gr/ypiresia-pliroforikis/.