Journal of AI

Volume: 8, **Issue No:** 1, January-December 2024, **Pages:** 61-82

Cybersecurity in The Health Sector in The Reality of Artificial Intelligence, And Information Security Conceptually

Muhammet Damar[1,2], Ahmet Özen[3], Ayşin Yılmaz[4]

[1] Dokuz Eylul University, Türkiye **Email**: muhammet.damar@deu.edu.tr **Orcid**: 0000-0002-3985-3073
[2] Upstream Lab, MAP, Li Ka Shing Knowledge Institute, Unity Health Toronto, Ontario, Canada
[3] Faculty of Economics and Administrative Sciences, Dokuz Eylul University, Türkiye. **Email**: ahmet.ozen@deu.edu.tr **Orcid**: 0000-0002-9635-5134
[4] Faculty of Economics and Administrative Sciences, Dokuz Eylul University, Türkiye. **Email**: aysin.yilmaz@ogr.deu.edu.tr **Orcid**: 0009-0002-0934-4670

Corresponding author: muhammet.damar@deu.edu.tr

Received: 07.04.2024 Accepted: 01.07.2024 Online: 06.07.2024 Published: 31.12.2024

Review Article

Abstract

Healthcare service delivery, especially in terms of safeguarding personal data, requires ensuring the confidentiality of information. In this regard, establishing cybersecurity systems that ensure information security is highly necessary. The rapid advancement of technologies increases the likelihood of cyberattacks, and particularly, AI-supported threats can cause serious harm in service delivery. In the current era, attacks not only come from humans but also from AI tools, posing threats to information se curity. Considering that AI technology is expected to further advance in the future, it's evident that this technology could become even more menacing. This is especially pertinent to the healthcare sector. Cyberattacks can lead to breaches in healthcare system data and disrupt service delivery to the extent of paralyzing the healthcare system. Our study, which includes case examples, is a compilation-type research. Within the scope of our research, searches were conducted using the keywords healthcare sector, information security, and cybersecurity on Google Scholar and Web of Science. The most current topic headings intersecting information security with the healthcare sector were examined based on the articles found on the subject. Our study evaluates the following topics in order: information and cyber security concepts, cyber threats and public services, electronic health records and security, major cyber-attacks in the health sector, why healthcare data is attractive for cyberattacks, information security in the artificial intelligence era, and information security policies for Türkiye and other countries in the world. Ransomware holds a significant place among cyberattacks. Therefore, users within the healthcare system are advised to pay particular atte ntion to this issue. Attacks generally occur via email, starting with enticing the user into a cyber-threat through email. Artificial intelligence can also be used to get rid of such spam mails. Hence, it is strongly recommended that users in the healthcare sector undergo training on this matter. These trainings should be conducted regularly and continuously, with the institution's IT center offering an institutional approach in this regard.

Keywords: *Cyber attacks in health sector, health information, security policies, health sector, artificial intelligence, cyber threats, cyber security*

Cite this paper (APA)

Damar, M., Özen, A., Yılmaz, A. (2024). Cybersecurity in The Health Sector in The Reality of Artificial Intelligence, And Information Security Conceptuall. Journal of AI. 8(1), 61-82. Doi: 10.61969/jai.1466340

1. INTRODUCTION

In today's world, the widespread adoption of information technologies and their integration into various fields are changing the delivery styles of traditional public services and facilitating human life by providing practical opportunities (Cordella & Iannacci, 2010; Rosacker & Olson, 2008; Lindgren & Jansson, 2013). The rapid transformation in information and communication technologies significantly impacts the healthcare sector, as in all other domains (Iyanna et al., 2022; Herrmann et al., 2018). With advancements in information technologies, significant changes and transformations have occurred in the healthcare sector (Yılmaz et al., 2021; Iyanna et al., 2022). Moreover, with the influx of large amounts of data from many different systems, the role of data analytics in health informatics has increased in recent years (Galetsi et al., 2020; Jee & Kim, 2013). This has also led to an increased interest in building analytical, data-driven models based on machine learning in health informatics (Ravì et al., 2016). This has further increased the importance of concepts such as machine learning or artificial intelligence for the healthcare sector (Schwalbe & Wahl, 2020; Ali et al., 2023). Particularly, new technologies and methods enable improvements in treatment processes, communication with patients, processes related to health maintenance, and managerial processes of healthcare institutions (Ali et al., 2023). The rapidly evolving broadband internet and mobile connectivity solutions have virtualized processes such as appointments, follow-ups, and reporting in healthcare services, while cloud computing has overcome physical constraints for storing such data and similar information (Akalın & Veranyurt, 2020). However, developments in information and communication technologies are leading to an increasing number of attacks on individuals' privacy and data confidentiality.

In the context of data security, the security of Electronic Health Records (EHRs) is the first thing that comes to mind (Berber et al., 2009). Electronic health records consist of data used to automate a doctor's workflow (Öğütçü et al., 2011). According to Häyrinen et al. (2008), the concept of EHR encompasses a wide range of information systems, from the compilation of patient data from single departments to the long-term aggregation of patient records. In EHR systems, various data elements are documented, including daily schedules, medication administration records, physical assessments, admission nurse notes, nursing care plans, referrals, current complaints (such as symptoms), past medical histories, lifestyles, physical examinations, diagnoses, tests, procedures, treatments, medication therapies, discharge summaries, histories, logs, issues, findings, and vaccinations. In the future, it will be necessary to incorporate different types of standardized tools, electronic consultations, and nursing documentation systems into EHR systems.

All organizations must take active steps to protect the security and integrity of information resources, and this strategy is nowhere as critical as in hospitals, where issues of information accuracy and patient confidentiality are paramount (Stahl et al., 2012). The possibility of storing health information in electronic format increases concerns about patient privacy and data security. Therefore, any endeavor to implement computerized health service information systems must ensure the adequate protection of patient information privacy and integrity (Smith & Eloff, 1999). Naturally, the primary objective is to protect and securely store the privacy information of patients (Stahl et al., 2012). To ensure information and data security in healthcare services, the establishment of information security systems prevents unauthorized access to personal data, thus safeguarding data privacy. Like all data in electronic environments, security measures must be taken to mitigate risks that threaten personal health information (Par & Soysal, 2011).

The widespread use of Artificial Intelligence (AI) technologies in the healthcare sector makes information security and cyber security issues even more important. While the digitization of health data and the use of artificial intelligence algorithms enable more effective and efficient delivery of healthcare services, it also creates important responsibilities for the security of this data. AI can influence the field of information security both positively and negatively. Advanced threat detection and prevention, the evolution of malware and attacks, personal data privacy and security, AI-based social engineering, and AI-supported security

solutions can be cited as positive examples. AI can be utilized to provide more effective and rapid responses in the field of information security. For instance, AI-based security systems that automatically detect and prevent attacks can be developed. However, in malicious applications, the opposite can occur. In conclusion, AI presents both new opportunities and new risks in the field of information security. Therefore, it is important for security experts to understand both the positive and negative aspects of AI technologies and to ensure information security by taking appropriate security measures.

Security is a pivotal concern in healthcare information systems, as most aspects of security become crucial and even critically important when processing healthcare information (Gritzalis, 1998). Previously, a data breach, a missing paper document, or a stolen computer would affect tens or thousands of patients, but today, as this content is digitized and accessible over many networks, a cyberattack has the capacity to harm millions of patients (Ganai et al., 2022). Although many studies have been conducted on the use of AI in the healthcare sector, it has been observed that there is a lack of research on information security and cybersecurity focusing on the healthcare sector in the context of AI. Limited research has focused on examining information security risks in the healthcare sector (Appari & Johnson, 2010). In this context our study evaluates the following topics in order: information and cyber security concepts, cyber threats and public services, electronic health records and security, major cyber-attacks in the health sector, why healthcare data is attractive for cyberattacks, information security in the artificial intelligence era, and information security policies for Türkiye and other countries in the world. The concept of information security within the healthcare sector has been comprehensively evaluated, as evident from the topic headings. As detailed in the methodology section, sources obtained through Google Scholar and Web of Science have been examined through abstracts and titles, followed by full-text readings, to discuss various approaches to information security in the healthcare sector. This topic has been thoroughly debated and evaluated within the framework of the literature. Our research aims to contribute to the literature by providing a comprehensive literature review in this regard.

2. METHODOLOGY

In our study, data security has been centered on from the perspective of the healthcare sector, and the issue of data privacy has been evaluated in detail. In this context, assessments have been made on how healthcare data can be protected using findings obtained through national and international literature research. This study addresses information security and cybersecurity issues in the health sector using literature review and conceptual analysis methods. Information from the relevant literature will be used to build a conceptual framework and evaluate current policy practices. Indeed, searches were conducted through Google Scholar and Web of Science using keywords such as healthcare sector, information security, artificial intelligence, and cybersecurity. The articles obtained through the relevant keywords on Google Scholar were accessed one by one and the full text of the articles deemed appropriate were accessed through the title and abstract. By reading the full texts, the titles that would contribute to our article were added to the article content and discussed. In the Web of Science search, a topic search was performed. The main search words used were “ts=(("health sector" and "artificial intelligence") or ("health informatics" and "artificial intelligence") or ("cyber security" and "artificial intelligence") or ("information security" and "artificial intelligence") or ("cyber security" and "health informatics"))”. The studies with the highest number of citations in the obtained data set were primarily focused on. Articles and other internet sources obtained within the scope of the topic are being evaluated in the research regarding the connection between information security and the healthcare sector. Our research is of a review type. As mentioned above, the titles and abstracts of the articles obtained from the search with the keywords on the relevant subject on Google Scholar and Web of Science were first accessed, and the full texts of the relevant articles were accessed. By reading within the subject, the issue of information security in the health sector in the reality of artificial intelligence was conceptually revealed with the subjective evaluation of the authors.

3. INFORMATION SECURITY AND CYBER SECURITY IN CONCEPTUAL TERMS

3.1 Information Security Concept

Information security is the set of measures taken to ensure the confidentiality, integrity and accessibility of information. This concept aims to control access to information and protect against malicious attacks with the use of information technologies. Information can exist in various forms. It can be written or printed on paper, stored electronically, shown in films, transmitted via electronic devices or mail, or spoken in conversations. Regardless of the type of information, it should always be appropriately protected. At this point, information security, conceptually expressed, involves implementing a set of controls including policies, procedures, processes, software and hardware functions, and organizational structures to protect information (ISO/IEC, 2005).

According to the definition provided by the National Security Telecommunications and Information Systems Security Committee, information security is the protection of all hardware and software systems that handle, transmit, store, or use information. Technically speaking, information security aims to safeguard the accuracy, availability, confidentiality, authenticity, integrity, and ownership of information. Of course, there are many threats to information security. These include, in order, unauthorized access to information, destruction of information, and alteration of information (Huang et al., 2010). In addition, Shchavinsky et al. (2023) also addressed the issue of the need for continuous development and improvement of the practical skills of cybersecurity professionals due to the continuous growth of threats to information and cybersecurity for organizations, businesses, society and government.

Within the historical development of information security, the McCumber Information Security Model stands out as a prominent framework for evaluating information security policies comprehensively. Since its inception in 1991, this model has remained valid and has served as the basis for subsequent models, addressing various dimensions of information security. The model encompasses three main elements: the characteristic, status, and security measures of information, inclusive of confidentiality, integrity, and availability. Confidentiality, the first element, refers to ensuring that information is accessible only to those authorized to access it. Integrity, the second element, pertains to maintaining the original state of information resources in any electronic environment or information center, ensuring that they remain unaltered by unauthorized individuals, thus preserving the integrity of the information. The third element, Availability, refers to accessibility and continuity, allowing users to access the information they need whenever they need it, provided they have the necessary authorization (Henkoğlu et al., 2013).

Since the implementation of health information systems, particularly considering the highly sensitive nature of their data, their security has been regarded as a significant concern. The possibility of storing health information electronically exacerbates concerns regarding patient privacy and data security (Smith & Eloff, 1999). Security, privacy, and access to personal data represent a critical area for the healthcare sector. Given that it serves a wide and large community, its importance in terms of information security is further heightened. It is perceived as a domain necessitating strategic management (Chiuchisan et al., 2017). Information security risks may include personnel leaving data assets unattended on-site, personnel losing a data asset, personnel sharing passwords to access patient data, personnel sending emails containing personal patient data to the wrong recipient, and unauthorized disclosure of data. Additionally, outsourcing data storage and processing processes to external servers for certain server services poses a significant information security risk. Emerging technologies such as cloud computing or RFID are prominent in this regard (Van Deursen et al., 2013). Gritzalis (1998) has viewed standardization as a significant tool for addressing the security gap in the healthcare sector.

3.2 Cyber Security Concept

In recent years, the terminology used to discuss the security aspects of digital devices and information has undergone significant changes. At the beginning of the century, the terms commonly used in this context were computer security, information technology security, or information security (Schatz et al., 2017). Indeed, in recent years, the term "cyber security" has been increasingly used in place of the previously mentioned terms. Of course, the widespread integration of the internet into various aspects of our lives has greatly influenced this shift.

Cybersecurity is an increasingly serious and complex issue at all levels (Caruson et al., 2012), requiring attention from all government levels (Chodakowska et al., 2022). In fact, cybersecurity is of paramount importance for maintaining business integrity, ensuring data security, and protecting cyber assets (Abdallah et al., 2021). Today, cybersecurity is considered one of the most significant socio-technological challenges faced by public institutions, crucial not only for the smooth functioning of government and local administrations but also for private companies using e-government services and the residents of relevant local administrations (Chodakowska et al., 2022).

Cyber security is the process of protecting computer systems, networks and other digital infrastructures from malicious attacks, data breaches and other threats. Cyber security is the set of measures that ensure the implementation of information security in the digital environment.

In a narrow sense, cybersecurity is the practice of protecting data and information resources. In a broader sense, it concerns the protection of digital content, information technology networks, business devices, and content transfer over the internet. The concept of cybersecurity emerged in the United States in the 1970s and spread worldwide by the late 1990s (Cavelty, 2010). Cybersecurity involves processes and technologies created to combat threats in cyberspace, primarily unauthorized access by cybercriminals, hackers, and terrorist hackers, aiming to protect computers, computer software, hardware, data, and networks from security vulnerabilities (Goutam, 2015). Cybersecurity is a term commonly used to protect against malware and hacker attacks (Bay, 2016). Indeed, cybersecurity and cyberspace are distinct concepts but closely related. Cybersecurity pertains to protecting internet-connected systems from cyberattacks, while cyberspace is the virtual realm used to store, share, and exchange information through the relevant physical infrastructure and network-connected systems. The place where internet activities occur is abstract and entirely virtual, serving as a medium for communication and information exchange. Therefore, cyberspace is a structure without boundaries that can expand rapidly without any political or physical constraints (Goutam, 2015).

The healthcare sector implements electronic health records for information sharing among relevant healthcare providers, updates them, establishes intranets, and also utilizes the internet to disseminate health-related information. Consequently, healthcare information systems become an integral part of all aspects of healthcare delivery (Smith & Eloff, 1999). Cybersecurity has various expectations in the health and medical sectors. Today's medical fields employ digital communication and documentation tools. It is imperative to ensure the highest possible protection of such documents. Healthcare systems possess sensitive information, necessitating the protection of these sensitive data from cyber threats (Pawar et al., 2024).

The healthcare sector is one of the most critical sectors for the Internet of Things (IoT). With the implementation of the Internet of Things in the healthcare sector, individuals have had to make efforts to develop platforms at both the hardware and software levels. Every sector is moving towards IoT integration, and this can create security vulnerabilities and threats in the healthcare sector. Ganai et al. (2022) statet that IoT is widely used in the healthcare sector to enhance service security. Similarly, IoT devices can also pose a

security vulnerability and are increasingly prevalent in the healthcare sector, as in all sectors. The presence of an IoT device in a healthcare environment can provide an access point for illegal hacking attacks, thus creating a security loophole. The European legal framework applicable to IoT technologies in the healthcare sector is not clearly defined. Only two regulations, namely the General Data Protection Regulation (GDPR) and the Medical Device Regulation (MDR), are available (Casarosa, 2024).

3.2.1 Cyber Threats

Cyber threats are malicious activities that aim to damage computer systems and networks, steal data, and cause service interruptions. Cyber threats can occur through malware, ransomware, information leaks and other attack techniques (Aydın, 2020). Cybersecurity aims to protect against major cyber threats through internet-connected systems, including software, hardware, and data. These threats can be outlined as follows (Seemma et al., 2018; Goutam, 2015):

- *Cyber Terrorism*: These are attacks carried out by terrorist groups utilizing advancements in information technology to target computer systems, networks, and telecommunication infrastructures with the aim of advancing their political agendas.
- *Cyber Warfare*: This involves nation-states utilizing information technologies to infiltrate another nation's networks and cause harm. Cyber warfare is carried out by well-trained hackers with expertise in computer networks. In this type of cyber attack, networks are not shut down but are manipulated in ways that jeopardize the security of valuable data, disrupt infrastructure services, hinder trade, and sever communication channels.
- *Cyber Espionage*: This is the use of information technologies to obtain confidential information without the consent of individuals. It is the most commonly employed method for gaining economic, strategic, and military advantages. It is typically carried out using malicious software and hacking techniques.
- *Cyber Stalking*: This is a frequently conducted action aimed at forcibly intruding into individuals' personal lives to create anxiety, distress, and fear. Cyber stalkers take advantage of the anonymity of the internet to continue their activities without being detected. Cyber stalking, as it leads to psychological harassment of individuals, is also referred to as "psychological harassment" or "psychological terrorism."
- *Intellectual Property Theft*: This involves the theft of intellectual property, which includes new research, innovations, methods, formulas, or models with economic value, through cyberattacks.
- *Salami Attack*: In this type of cyberattack, cybercriminals or attackers steal small amounts of money from various bank accounts to accumulate substantial sums.
- *Identity Theft*: This is a type of cyberattack where an individual's important information, such as address, name, or credit card number, is stolen, allowing the perpetrator to impersonate that individual and commit crimes in their name.
- *Distributed Denial of Service (DDoS) Attack*: This involves suspending or temporarily interrupting services, rendering servers, computers, or network resources unavailable to authorized users.

3.2.2 Risks Posed by Cyber Threats to Public Services

As public services become increasingly digitalized, the risks of cyber attacks also escalate, potentially leading to serious disruptions in public services (Preis & Susskind, 2022). Indeed, the number of reported cybersecurity incidents and cyber attacks targeting government agencies continues to rise each year (Chałubińska-Jentkiewicz, 2021). However, despite cybersecurity being one of the most significant challenges

facing governments today, visibility and public awareness remain limited (Bruijn & Janssen, 2017).

Cyber threats in public services can threaten the security and well-being of society. In particular, critical infrastructures such as healthcare can become the target of cyber-attacks and cause serious damage. Public institutions are responsible for ensuring the security of information technology networks and systems (Chałubińska-Jentkiewicz, 2021). The following factors should not be overlooked to ensure information security (ISO/IEC, 2005):

a) Establishing a security policy that reflects the organization's objectives,

b) Achieving a corporate approach to implementing, monitoring, improving, and sustaining information security,

c) Ensuring support and commitment from management at all levels,

d) Understanding information security requirements, risk management, and risk assessment,

e) Effectively conveying information security to all employees, managers, and other relevant parties to raise awareness,

f) Distributing guides on information security standards and policies,

g) Allocating funds to information security management activities,

h) Increasing awareness of information security through appropriate education and training,

i) Establishing an effective and efficient incident management process for information security.

4. ELECTRONIC HEALTH RECORDS AND HEALTH DATA

Electronic health records (EHRs) and health data form an important part of digitalization in the healthcare sector. EHRs digitally store patients' medical histories, diagnoses, treatments and other health information. Health data refers to all the information contained in these records and is an important source for the training and implementation of AI algorithms.

According to the definition provided by the Healthcare Information and Management Systems Society (HIMSS), EHRs are longitudinal electronic records of patient health information generated by one or more encounters in any care delivery setting. These records include the patient's gender, developmental notes, issues, treatments, vital signs, medical history, immunizations, laboratory data, and radiology reports. Electronic health records automate and streamline the doctor's workflow, making it more efficient (Öğütçü et al., 2011).

In private or public healthcare institutions, information about patients' medical histories, test results, diagnoses, treatments, and their durations are stored in digital format (Dülger, 2015). Access to patients' past diagnoses and treatments enables physicians to make accurate diagnoses and perform interventions more quickly and with less risk. As expressed in healthcare research, the accessibility of patient information provides significant benefits (Küzeci, 2019). Personal health data recorded in the system are shared among different institutions, allowing multiple individuals to access patient information (Yılmaz et al., 2021).

Electronic health record systems contain health data classified as sensitive information, encompassing individuals' most private details. When digitized, these data become useful for analysis and visualization, thereby creating new ways to provide better insights into a patient's condition and potential for improved decision-making. The digitization of healthcare services can be defined in four stages (Gopal et al., 2019):

- First Stage: At this stage, patient data is still recorded in paper-based format. This significantly limits the useful analytics of the information and restricts the efficient use of resources.

- Second Stage: In the second stage, the utilization of data begins. However, despite the acceleration of digitization in healthcare data, paper-based record-keeping still largely exists. Therefore, at this stage, opportunities for researching and analyzing the information are limited.
- Third Stage: The third stage sees full implementation of digitization. In this regard, organizations make healthcare services smarter by implementing analytics, next-generation data generation, Artificial Intelligence (AI), Machine Learning (ML) technologies, along with new service models aimed at improving business performance.
- Fourth Stage: At this stage, the healthcare system adopts a value-based healthcare approach rather than a fee-for-service or per capita payment approach, focusing on the value of healthcare services rather than the quantity.

The establishment of a rich health data foundation and achieving digital transformation in healthcare services are made possible through the use of advanced technologies such as analytics, portability, wearability, cloud computing, Machine Learning (ML), Internet of Things (IoT), and Artificial Intelligence (AI). For instance, the utilization of wearable compact devices that provide information to users via physical input or voice commands and assist in user interaction enables a continuous flow of data regarding individuals' physiology and kinesiology. As a result, self-monitoring of health conditions such as hypertension and stress becomes feasible, aiding in their prevention (Iqbal et al., 2016).

Another digital application is mobile health services. Mobile health (mHealth) involves the use of mobile devices to collect real-time health data from patients, with the collected data being stored and maintained on internet-connected network servers. Various heterogeneous groups such as hospitals and health insurance companies can access this data. These data are utilized by doctors to monitor, diagnose, and treat patients' conditions. With the integration of mobile health devices into the patient's environment, health abnormalities can be monitored simultaneously (Almotiri et al., 2016).

Cloud-based systems also stand out in digital applications. In areas where digital infrastructure is insufficient, cloud computing is a proven low-cost method that offers interoperability and scalability. Cloud-based platforms transmit data to cloud-based servers when the internet is disrupted, storing the data. This allows providers not only to monitor patients' conditions but also facilitates data sharing among providers. Cloud-based systems, especially those operable on phones, assist healthcare professionals in monitoring patients' conditions, providing them with an effective roadmap for decision-making, and streamlining workflow (Perednia et al., 1995).

Thanks to the digital health applications mentioned above, health data is continuously increasing. Indeed, health data accounts for nearly 30% of the total data volume worldwide. For each patient, thousands of files and data fields describing their health status are collected. A single patient generates about 80 megabytes of health data by utilizing electronic health record data. The largest sources of data used for diagnosis are images, proteomic information, and omics data (such as full genome sequence data). Developments in the Internet of Things, mobile technology, and sensors enable additional diagnostic information from connected medical devices and interpretation of Patient-Reported Outcomes from smartphones (Gopal et al., 2019).

Health data can be used for analyses that describe patients' characteristics. Analyzing rich data enables more diversified segmentation. For example, populations at high risk of future health issues (e.g., diabetes or cardiovascular events) can be identified (Gellerstedt, 2016).

4.1 Information Security in Healthcare in the Era of Artificial Intelligence

In today's world, information security has evolved from the mainframe era to the complex internet environment. Security issues now require a more coordinated and focused effort from national and

international communities, governments, and the private sector. Therefore, it is critically important to continue strengthening technologies to overcome new challenges in information security (Dlamini, 2009).

Artificial intelligence refers to the simulation of human intelligence in machines. AI is revolutionizing healthcare services and becoming a transformative force (Mukherjee et al., 2022). Artificial intelligence plays an important role in the healthcare sector in improving healthcare services and diagnosing and treating diseases. Khan et al. (2023) stated that artificial intelligence has the potential to make significant progress towards the goal of making healthcare services more personalized, predictive, preventive, and interactive. Artificial intelligence can be utilized for diagnosis, drug development, personalized treatment, gene editing, disease prediction, and many other purposes. It aids in improving healthcare services by benefiting medical professionals, hospitals, and patients (Chikhaoui et al., 2022). Alugubelli (2016) stated that the rise of artificial intelligence has brought about a positive change in the sector by providing accurate data-driven decisions. In the healthcare sector, data obtained from large systems can be used for the early detection of chronic diseases, including cancer, diabetes, and cardiovascular diseases. However, the security of health data obtained through AI applications is a serious concern. Therefore, information security policies and practices are gaining importance in the healthcare sector in the era of AI. Machine learning has also had a significant impact in the healthcare sector alongside artificial intelligence. Machine learning is described as a technique used in the healthcare system to assist medical practitioners in patient care and clinical data management (Khan et al.,2023).

Deep learning, a technique based on artificial neural networks, has emerged in recent years as a powerful tool for machine learning. Deep learning also holds great promise for reshaping the future of artificial intelligence. Rapid advances in computational power, fast data storage and parallel processing capabilities have also contributed to a faster adoption of AI technology, with capabilities such as high-level features for predictive power and automatic optimization from input data (Ravì et al., 2016).

In the current era, attacks against information security can be carried out not only by humans but also by artificial intelligence tools. Moreover, considering that artificial intelligence technology is expected to advance even further in the future, it is evident that this technology could become even more threatening. Of course, this situation is even more relevant to the healthcare sector. The following are the types of impacts that may occur due to the misuse of healthcare data by artificial intelligence:

- *Privacy Violations*: Healthcare data contains personal and sensitive information. Artificial intelligence algorithms may encounter challenges in ensuring privacy while analyzing this data. This situation can lead to unauthorized access to the data and its malicious use.
- *Discrimination and Bias*: Artificial intelligence systems can learn biases from the datasets or create new forms of discrimination. For example, inadequate representation of certain ethnic groups or genders in some healthcare datasets may result in AI models failing to make accurate diagnoses and providing incorrect treatment recommendations for these groups.
- *False Results and Misdiagnoses*: AI models may produce incorrect results based on the data, leading to misdiagnoses, unnecessary treatments, or potentially harmful interventions.
- *Misuse and Harassment*: Artificial intelligence has the potential to misuse healthcare data and harass individuals. For instance, malicious actors who leak or gain unauthorized access to this data can pose threats based on personal information or exploit personal data.
- *Security Vulnerabilities*: The security of artificial intelligence systems can be challenging. These systems may be targeted by malicious actors for data manipulation or injection of malicious software, among other attacks.

To overcome these risks, strict security protocols and legal regulations are necessary for the collection, storage, and analysis of healthcare data. Additionally, transparency and accountability are essential during the training and evaluation of artificial intelligence algorithms. It is also crucial to design and implement artificial intelligence systems in accordance with ethical and justice principles. In this way, the risk of misuse of healthcare data by artificial intelligence can be reduced or prevented.

4.2 Major Cyber Attacks in the Healthcare Industry Around the World

The healthcare industry worldwide has become a target for cyber attackers. Cyber-attacks on major hospitals and healthcare organizations have caused serious consequences such as leakage of patients' health information, service interruptions and ransom demands. The healthcare sector has become increasingly vulnerable to cyber-attacks in recent years. Here are some major cyber-attacks targeting the healthcare sector in history:

- Stuxnet Attack (2010): Stuxnet was a cyber-attack targeting Iran's nuclear program, but one of its targets was also the control systems of medical devices associated with nuclear facilities in Iran. This attack had the potential to take control of and disable medical devices, particularly targeting vulnerabilities in industrial control systems used by Siemens, aiming to cause serious damage to targeted facilities (ELFANET, 2024).
- Tricare (2011): In late 2011, Science Applications International Corporation (SAIC), the federal government's military healthcare provider, announced a data breach affecting approximately 4.9 million military clinic and hospital patients registered with TRICARE. The data was stolen from a SAIC employee's car, impacting active and retired military personnel as well as their families. While no financial data was involved, the exposed sensitive information included Social Security numbers, phone numbers, home addresses, and other personal data (Digital Guardian, 2024).
- Advocate Health Care Data Breach (2013): Advocate Health Care fell victim to a series of data breaches following the theft of four personal computers storing unencrypted medical information of 4.03 million patients. The failure to implement the most basic cybersecurity practice of data encryption was a blatant violation of data protection standards outlined in the Health Insurance Portability and Accountability Act. As a consequence of such a misstep, the relevant institution was fined $5.55 million to send a strong message to other healthcare entities about the consequences of such lapses in security (Upguard, 2024).
- Premera Blue Cross (2014): In 2014, Premera Blue Cross experienced a significant data breach that led to unauthorized access to sensitive personal and medical information of millions of individuals, potentially putting them at risk. Regarded as one of the largest healthcare data breaches in history, the breach began with the simple opening of an email by an employee. Premera remained unaware of the breach for eight months. The attack resulted in a $74 million loss and impacted data of 11 million patients (Arcticwolf, 2023).
- Banner Health (2016): In 2016, hackers used malware to breach the payment processing system of Banner Health's food and beverage outlets. Subsequently, they utilized the system as a gateway to Banner Health's network and eventually gained access to servers containing patient data. The cyberattack went unnoticed for almost a month. The stolen data included highly sensitive information such as Social Security numbers, service and request dates, health insurance details, and more. The attack resulted in a $6 million loss and impacted data of 3.7 million patients (Arcticwolf, 2023).
- WannaCry Attack (2017): WannaCry can be cited as an example of ransomware, a type of malicious

software used by cybercriminals to extort money. It was a large-scale ransomware attack that affected numerous organizations worldwide. The healthcare sector, including hospitals and healthcare institutions, was significantly impacted by the attack. Many hospitals and clinics had their systems locked, disrupting patient care and medical services. As a result, the company faced significant financial and reputational repercussions, including a hefty fine levied by the Department of Health and Human Services' Office for Civil Rights (OCR). Responsible for enforcing the Health Insurance Portability and Accountability Act's (HIPAA) implementation, the OCR found that Premera violated many provisions of the HIPAA Security Rule (Kaspersky, 2024).

- Ryuk Attacks (2018-present): Ryuk is a ransomware attributed to the cybercriminal group WIZARD SPIDER, which poses a threat to governments, universities, healthcare, manufacturing, and technology organizations. These attacks target hospitals and healthcare systems, posing serious consequences that endanger patient care and disrupt healthcare services (Trend Micro, 2024).
- American Medical Collection Agency (2019): The data breach of the American Medical Collection Agency (AMCA) raised significant concerns in the healthcare sector. In June 2019, it was revealed that the third-party billing and collection services provider AMCA had caused a major data breach jeopardizing the personal and financial information of millions of individuals. This breach had serious consequences for both patients and healthcare service providers. The compromised data included names, addresses, birth dates, social security numbers, and payment card information (Getoppos, 2024). With the potential exposure of this sensitive information to unauthorized parties, individuals faced risks of identity theft, fraud, and other malicious activities. Consequently, this sensitive incident resulted in significant reputational damage and financial loss for the company. The attack is estimated to have caused $21 million in damages and affected the data of 21 million patients (Arcticwolf, 2023).
- University of California, Los Angeles (UCLA) Health (2023): The 2023 ransomware attack on UCLA Health was a significant cybersecurity incident that occurred at the University of California in Los Angeles. Ransomware is a type of malicious software that encrypts the victim's files and demands ransom payment in exchange for the decryption key. The impact of the ransomware attack was felt across the university, affecting critical systems and databases of various departments and services, leading to disruptions (Getoppos, 2024). The attack is estimated to have caused $7.5 million in damages and affected the data of 4.5 million patients (Arcticwolf, 2023).

These cyber-attacks have highlighted the cybersecurity vulnerabilities in the healthcare sector and underscored the need for healthcare organizations to strengthen their cybersecurity. Particularly, addressing issues such as the privacy of patient data, security of medical devices, and continuity of healthcare systems is crucial. Hospitals may have numerous entry points that hackers can exploit. Outdated computer systems, weak passwords, unpatched or outdated software, and stolen accounts from old computers can all play a role in this vulnerability. It should be noted that cybercriminals exploit any security gap to infiltrate and harm the hospital's network, and the most effective way to overcome this is through the implementation of an effective corporate information security policy and ensuring its sustainability.

4.3 Why Healthcare and Health Data Are Attractive for Cyber Attacks

Health records are significant and vulnerable, leading hackers to frequently target these records during data breaches. The lack of standardized guidelines for the ethical use of artificial intelligence and machine learning in healthcare services exacerbates this situation (Khan et al., 2023). The healthcare sector provides access to large amounts of sensitive health data, making it valuable targets for cyber attackers. Health data includes personal diagnostic information, medical histories and other sensitive information, making it attractive for

malicious uses. The healthcare sector provides access to large amounts of sensitive health data, making it valuable Hospitals, in particular, are susceptible to cyberattacks because disruptions in their operations can pose life-threatening risks to patients, making them more likely to pay ransoms demanded by hackers. Additionally, budget constraints often leave healthcare facilities with limited resources and outdated IT infrastructure, making them more vulnerable to cyber threats. Furthermore, the increasing use of connected IoT devices in healthcare introduces new attack vectors for hackers. Insecurely connected medical devices can serve as entry points for cybercriminals to exploit security vulnerabilities and launch cyberattacks (Getoppos, 2024).

The most effective way to address this is for healthcare institutions to implement a robust information security policy within their organizations. In this process, the active participation of all healthcare personnel is crucial and of paramount importance. In a sustainable security policy, the responsibility does not solely fall on the information technology department or units. Certainly, these units have a critical role in ensuring the effective implementation of the existing or newly formulated information security policy. However, all personnel throughout the healthcare institution are actively involved in the information security policy. There are various aspects that users need to be mindful of, from the use of emails to the usage of portable storage devices. Therefore, periodic training sessions, sustainable and well-planned information security policies, and ideally accreditation by an information security institution for ISO27001 or similar standards are also recommended.

5. INFORMATION SECURITY POLICY PRACTICES IN HEALTH

With the advancement of technology, strides taken in all these healthcare services have also increased some of the risks caused by technology. This has led to the commodification of rights and the multi-dimensional nature of the relationship between physicians and patients. In order to provide better healthcare services in this regard, providing access to individuals' health data requires careful protection of health-related data seen as sensitive personal information. Security measures against risks threatening personal health information have become mandatory. Personal health information encompasses all health information acquired from before a person's birth to after their death. The technologies have heightened the risks of integrity, confidentiality, and accessibility of health information, endangering its security. Due to the primacy of privacy in personal health data, measures have been taken to minimize risks (Öztürk et al., 2014).

For ensuring security in information technology and information systems, countries develop information security policies. An information security policy is considered an increasingly important document that encompasses a series of security measures. The policy serves as a guiding document about the tools used in information security management and the desired outcomes. Additionally, it outlines the organization's approach to managing information security (Stahl et al., 2012).

5.1 Health Information Security Policies in Some Countries

Different countries have developed various policies and guidelines on health information security. These policies include various measures to ensure the security and privacy of health data. The World Health Organization has further developed the Helsinki Declaration, originally published in 1964, to express ethical principles in medical research and provide guidance to all participants. According to this declaration, "The dignity, privacy, and confidentiality of research subjects must always be respected. Every effort should be made to protect the privacy and confidentiality of subjects, minimize the impact of research on their physical and mental integrity and personality, and respect their integrity and personality". Accordingly, in the United States, national standards were established with the Health Insurance Portability and Accountability Act (HIPAA) enacted in 1996 for the storage of individuals' medical data and other personal health information. This national standard aims to reduce the misuse of data in the healthcare sector and protect the confidential

information of US citizens (Uysal & Yorulmaz, 2018).

In 1999, the Institute of Medicine (IOM) in the United States published a report titled "To Err is Human: Building a Safer System," emphasizing the importance of ensuring patient safety in the healthcare sector. The report recommended establishing a center for patient safety, creating a reporting system nationwide, developing patient safety programs, and setting performance standards. It highlighted that the existing healthcare delivery organization fails to provide effective, safe, and efficient healthcare delivery to patients. Therefore, it underscored the need for restructuring healthcare delivery approaches and organizational structures to align with new goals (Korkmaz, 2018).

Building on the recommendations of the IOM report, the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) initiated accreditation services to healthcare organizations worldwide in collaboration with the Joint Commission International (JCI) to implement patient safety goals outside the United States. JCI annually publishes and revises the International Patient Safety Goals (IPSG) with the guidance of an expert group. The goals, initially published in 2007 and updated in 2014, include initiatives such as verifying patient identity, ensuring effective communication, and promoting safety in the use of high-alert medications (Korkmaz, 2018).

In the United Kingdom, the British Standard BS-7799, which was significantly revised in 1999, was implemented to address health information security. This standard is a two-part framework that establishes, regulates, and documents security controls to protect the accuracy, confidentiality, and accessibility of information assets. The first part of the initial version published in 1999 describes working principles for information security, while the second part focuses on planning information security management systems and certification for such systems (Gerçeker, 2012). Another British Standard for information security management systems in the UK is BS7799-3:2005, titled "Rules for Information Security Management System Risk Management." This standard was developed to promote the adoption of the standard in small, medium, or large organizations. Its content includes topics such as identifying, assessing, monitoring, and controlling risks (Vural & Sağıroğlu, 2008).

The European Union adopts a method based on identifying threats and risks when formulating information security policies. Following analyses, numerous threats related to technology are identified, and the established policies are enacted into law and implemented. During the preparation phase of information policies, the main risks and threats are classified under three main headings. These were categorized by Henkoğlu & Yılmaz (2013) as unauthorized access to and intrusion into information systems, system disruption, obstruction, alteration, or destruction of data, and finally identity theft and misuse of personal data. The Luxembourg Declaration on Patient Safety, published in 2005, made the following recommendations to European Union institutions to preserve the confidentiality of patient records (European Union, 2005):

- Ensuring free, full access to patients' personal health data and ensuring the accuracy of the data.
- Implementing risk management routines taking into account the benefits of confidential reporting systems for potential risks.
- Promoting the use of new technologies, such as electronic health records.
- Establishing national forums with participation from relevant stakeholders to discuss national activities and patient safety.
- Ensuring the safe use of new surgical techniques and medical technologies.
- Integrating integrated procedures into the ongoing education of healthcare professionals, including continuous learning, a culture of patient safety, and improvement.

5.2 Health Information Security Policies in Türkiye

In Türkiye, reforms in the healthcare sector aimed at establishing health information systems began in the 1990s and gained momentum in the 2000s. The establishment of the health information system was addressed in the health sector section of the Eighth Five-Year Development Plan covering the years 2001-2005, stating that "All levels of healthcare service delivery will be improved in terms of human resources, infrastructure, management, and technology, and a health information system will be established." Additionally, the plan emphasized the need for establishing information infrastructure and setting policies in the public sector in line with the new role of the public in the information age, ensuring that information held by the public sector is disseminated to the public in accordance with principles of transparency and openness. In alignment with these principles, an action plan was prepared in 2003 (Sağlık Bakanlığı, 2004).

In 2003, the 58th Government prepared an Emergency Action Plan aimed at ensuring the provision of quality, cost-effective, continuous, widespread, and community-oriented healthcare services. The health reforms outlined in the plan were announced by the Ministry of Health under the name "Health Transformation Program" later that year, emphasizing the establishment of a health information system and access to effective information in decision-making processes as a significant component of digitalization in healthcare. Within this framework, fifteen objectives were listed for the development of the health information system as part of the e-Health project in 2004. These identified objectives were considered crucial for the establishment of the National Health System (Avaner & Fedai, 2017).

The Health Transformation Program envisaged eight fundamental components: (1) A Planning and Supervisory Health Ministry, (2) Universal Health Insurance that brings everyone under one roof, (3) A widespread, easily accessible, and friendly Healthcare Service System, (4) Health Human Resources Equipped with Information and Skills, Highly Motivated, (5) Education and Scientific Institutions Supporting the System, (6) Quality and Accreditation for Qualified and Effective Health Services to support the system, (7) Institutional Structuring in Rational Drug and Material Management, and (8) Access to Effective Information in Decision-Making - Health Information System. To ensure coordination and harmony among all these components, the establishment of an interconnected information system is required (Sağlık Bakanlığı, 2003).

In Türkiye, partial steps towards digital transformation have been taken by institutions through the implementation of the "E-Transformation Turkey" project, which binds public institutions affiliated with the Prime Ministry to its scope. Within the framework of the E-Transformation project, the Ministry of Health Project aims to ensure the security and continuity of financial, administrative, and clinical data shared in information systems, protect the institution's reputation and investments, and minimize legal risks arising from security breaches by establishing standards for information system security in all institutions affiliated with the Ministry of Health. The Ministry's information security policy consists of rules and methods established under 23 main headings, including antivirus systems, email security, and encryption (Marttin & Pehlivan, 2010). Within the framework of the National Health Information Systems established with the Health Transformation Program, there are applications such as the Basic Health Statistics Module, Hospital Information Management Systems, Core Resource Management System, and Family Medicine Information System under the name Health.net (Avaner & Fedai, 2017). Additionally, within the scope of the e-health project in the Health Transformation Program, various information systems such as e-Pulse, Telemedicine, and the Ministry of Health Communication Center (SABİM) are implemented (DPT, 2005). For example, Telemedicine enables the instant transfer of information between patients and healthcare providers, eliminating physical barriers (Perednia et al., 1995).

In addition to the activities carried out under the title of the Health Transformation Program in 2007, three

new headings were added. These headings are listed below (Akdağ, 2008):

- Development of the healthcare sector towards a better future and the implementation of healthy life programs.
- Activation of stakeholders and the establishment of multilateral health responsibility for collaboration between sectors.
- Provision of cross-border health services to enhance the country's strength internationally.

In Türkiye, personal health data is collected and commodified through the Ministry of Health, Private Health Insurance, and the Social Security Institution (SGK) as a result of the privatization of healthcare services under the Health Transformation Program. Initially, personal health data collected in the electronic record system called MEDULA, meaning Health Network, which was primarily accounting-oriented, became more comprehensive and widespread over time. Starting from December 1, 2013, the Biometric Identity Verification System, which utilizes methods such as facial recognition, fingerprinting, voice recognition, and retinal scanning for biologically and irreversibly identifying individuals, was made mandatory for use in private hospitals by the SGK (İzgi, 2014). Additionally, in 2014, the Information Security Policies Directive and Guide, focusing on information security in healthcare services, came into effect with the approval of the Ministry of Health. The objectives outlined in this directive are as follows (Öztürk, 2014):

- Taking measures to ensure security in the collection, reporting, and sharing of information falling within the scope of the Ministry of Health's responsibilities.
- Ensuring protection against all external and internal threats to the integrity, confidentiality, and accessibility of information.
- Preventing human-caused damages by increasing awareness of information security among all managers and technical personnel involved in work on information networks and systems.
- Providing a computing infrastructure with ensured integrity, confidentiality, and accessibility.
- Preventing information and data losses through the achievement of sustainability.

Under the provisions of the Law on Protection of Personal Data dated 2016, the Regulation on Personal Health Data has been enacted to regulate the procedures and principles to be followed in practices carried out by the units of the Ministry of Health and the service providers affiliated with them, aiming to ensure data security in healthcare services. According to this regulation, a registration and notification system is established to enable individuals to monitor their health status and to effectively conduct healthcare services. The regulation stipulates that past health data cannot be disclosed except in cases required for the provision of healthcare services. Healthcare service providers must take necessary technical, physical, and administrative measures to prevent unauthorized individuals from accessing personal data belonging to others in service areas such as counters. Access to health data by healthcare personnel is limited to what is necessary for the service. In the event of death, the health data of a deceased individual is preserved for 20 years, and the legal heirs of the deceased, upon presenting a certificate of inheritance, are authorized to obtain this data (Mevzuat Bilgi Sistemi, 2016).

6. CONCLUSIONS AND RECOMMENDATIONS

Health data is continuously increasing worldwide, posing a risk of being vulnerable to cyber-attacks by hackers. Indeed, cyber-attacks can be likened to hurricanes that devastate an entire city's critical infrastructure or paralyze a nation. The losses incurred can be significant for a country. Considering that one-third of the world's population is widely interconnected through various platforms, including public institutions and services, cybersecurity plays a critical role in all forms of digitalization. Therefore, information

security is of paramount importance for other services that are part of the digital transformation to perform their expected functions effectively and efficiently.

The increasing prevalence of viruses, spam, hackers, spyware, and numerous other threats to information security has led to millions of security issues. These problems result in companies suffering financial losses, human rights violations, and the collapse of entire information systems, causing serious impacts on society and the economy (Huang et al., 2010:221). Therefore, institutions holding health information data need to develop security software to protect against cyber-attacks and appoint individuals responsible for ensuring compliance with cybersecurity policies (Chatfield & Reddick, 2019). Additionally, a successful security system can be established through multiple security layers. These layers include physical security, personnel security, transaction security, communication security, network security, and data security (Goutam, 2015; Elattresh, 2022).

It is essential to recognize the intertwined nature of technology and information in healthcare and to continuously enhance security measures to safeguard information alongside technological advancements. Cyberattacks pose a significant threat to the healthcare sector, with hospitals being prime targets. Among the most prevalent threats are ransomware attacks, data breaches, and phishing attempts.

As evident, ransomware occupies a significant place among cyberattacks, particularly within the healthcare sector. Therefore, it is recommended that users within the healthcare system pay particular attention to this issue. Attacks typically commence through email methods, luring users into cyber threats via email. Therefore, it is strongly advised that users in the healthcare sector undergo training on this matter. These training sessions should be conducted regularly and continuously, with the institutional IT center providing a corporate approach in this regard. Additionally, users should promptly inform the IT department of any suspicious emails that may pose a threat.

Hospitals are prime targets for cybercriminals due to the wealth of valuable data they harbor, encompassing patients' personal and financial details, medical histories, and research findings. This data holds significant monetary value and thus makes healthcare facilities lucrative targets for cyberattacks. Factors contributing to such attacks include the critical nature of healthcare services, the multitude of entry points for exploitation, limited cybersecurity resources, and the proliferation of interconnected devices. To mitigate these risks and safeguard patients' sensitive information, healthcare organizations must implement robust security measures and enhance staff awareness. Investing in strong cybersecurity strategies is essential to protect sensitive data and ensure uninterrupted operation of critical systems. Although addressing this issue is complex, especially in developing countries, governments have a duty to find pragmatic solutions. Moreover, service providers should prioritize data protection, assess the security practices of third-party suppliers regularly, and take proactive measures to prevent future incidents. Above all, utmost care must be taken to safeguard patients' personal information.

ACKNOWLEDGEMENTS

M. Damar was supported by the Scientific and Technological Research Council of Türkiye (TUBITAK) under the TUBITAK 2219 International Postdoctoral Research Fellowship program. He would like to thank the Upstream Lab, MAP, Li Ka Shing Knowledge Institute at the University of Toronto for its excellent hospitality.

FUNDING

No funding

AUTHORS` CONTRIBUTIONS

All authors contributed equally to the manuscript and read and approved the final version of this paper.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

DATA AVAILABILITY

All relevant data are within the paper and its Supporting Information.

REFERENCES

Abdallah, Y. O., Shehab, E., & Al-Ashaab, A. (2021). Understanding Digital Transformation In The Manufacturing Industry: A Systematic Literature Review And Future Trends. Product: Management and Development, 19(1), 1-12.

Akalın, B., & Veranyurt, Ü. (2020). Sağlıkta Dijitalleşme Ve Yapay Zekâ. SDÜ Sağlık Yönetimi Dergisi, 2(2), 128-137.

Akdağ, R. (2008). Türkiye Sağlık Dönüşüm Programı ve Sağlık Hizmetleri Değerlendirme Raporu,1.Baskı, Ankara: Türkiye Cumhurieti Sağlık Bakanlığı.

Ali, O., Abdelbaki, W., Shrestha, A., Elbasi, E., Alryalat, M. A. A., & Dwivedi, Y. K. (2023). A systematic literature review of artificial intelligence in the healthcare sector: Benefits, challenges, methodologies, and functionalities. Journal of Innovation & Knowledge, 8(1), 100333.

Almotiri, S. H., Khan, M. A., & Alghamdi, M. A. (2016). Mobile Health (M-Health) System in The Context of IoT. In 2016 IEEE 4th International Conference On Future Internet of Things and Cloud Workshops (Ficloudw) (Pp. 39-42). IEE, 22-24 Aug. 2016 Vienna, Austria.

Alugubelli, R. (2016). Exploratory study of artificial intelligence in healthcare. International Journal of Innovations in Engineering Research and Technology, 3(1), 1-10.

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. International journal of Internet and enterprise management, 6(4), 279-314.

Arcticwolf, (2023). The Top 15 Healthcare Industry Cyber Attacks of the Past Decade. https://arcticwolf.com/resources/blog/top-healthcare-industry-cyberattacks/. Access date: 06/04/2024.

Avaner, T., & Fedai, R. (2017). Sağlik Hizmetlerinde Dijitalleşme: Sağlık Yönetiminde Bilgi Sistemlerinin Kullanilmasi. Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 22(Kayfor 15 Özel Sayı), 1533-1542.

Aydın, Ö. (2020). Bilgisayar dünyasında hile, ihlal ve siber saldırılar. In Eds. Talan, T., & Aktürk, C. Bilgisayar Bilimlerinde Teorik ve Uygulamalı Araştırmalar (pp. 29-60). Efe Akademi.

Berber, L. (2009). Kişisel Sağlık Verileri ve Mahremiyet. 6. Ulusal Tıp Bilişimi Kongresi (TurkMIA '2009). 12-15 Kasım 2009, Antalya, Türkiye.

Berber, L., Ülgü. M.M, & Er, C. (2009). Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği. İstanbul: İstanbul Bilgi Üniversitesi, Bilişim Teknoloji Uygulaması Hukuku Uygulama Araştırma Merkezi.

Caruson, K., Macmanus, S. A., & Mcphee, B. D. (2012). Cybersecurity Policy-Making at The Local Government Level: An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to Success. Journal of Homeland Security and Emergency Management, 9(2), 20120003. https://doi.org/10.1515/jhsem-

2012-0003

Casarosa, F. (2024). Cybersecurity of Internet of Things in the health sector: Understanding the applicable legal framework. Computer Law & Security Review, 53, 105982.

Cavelty, M. D. (2010). Cyber-Security. In The Routledge Handbook Of New Security Studies (pp. 154-162). Netherlands: Routledge.

Chałubińska-Jentkiewicz, K. (2021). Cybersecurity Policy. In K. Chałubińska-Jentkiewicz, In: Karpiuk, M. & Kostrubiec, J. (Eds.) The Legal Status Of Public Entities in The Field Of Cybersecurity in Poland. Maribor: Institute for Local Self-Government Maribor.

Chatfield, A. T., & Reddick, C. G. (2019). A Framework for Internet of Things-Enabled Smart Government: a Case of IoT Cybersecurity Policies and Use Cases in US Federal Government. Government Information Quarterly, 36(2), 346-357. https://doi.org/10.1016/j.giq.2018.09.007

Chikhaoui, E., Alajmi, A., & Larabi-Marie-Sainte, S. (2022). Artificial intelligence applications in healthcare sector: ethical and legal challenges. Emerging Science Journal, 6(4), 717-738.

Chiuchisan, I., Balan, D. G., Geman, O., Chiuchisan, I., & Gordin, I. (2017). A security approach for health care information systems. In 2017 E-health and bioengineering conference (EHB) (pp. 721-724). 22-24 June 2017, Bucharest, Romania.

Chodakowska, A., Kańduła, S., & Przybylska, J. (2022). Cybersecurity in The Local Government Sector in Poland: More Work Needs to Be Done: More Work Needs to Be Done. Lex Localis-Journal of Local Self-Government, 20(1), 161-192. https://doi.org/10.4335/m75jka54

Cordella, A., & Iannacci, F. (2010). Information systems in the public sector: The e-Government enactment framework. The Journal of Strategic Information Systems, 19(1), 52-66.

De Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies. Government Information Quarterly, 34(1), 1-7. https://doi.org/10.1016/j.giq.2017.02.007

Digital Guardian, (2024). Top 10 Biggest Healthcare Data Breaches of All Time. https://www.digitalguardian.com/dskb/top-10-biggest-healthcare-data-breaches-all-time. Access date: 06/04/2024.

Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2009). Information Security: The Moving Target. Computers & Security, 28(3-4),189-198.

DPT, (2005). E-Devlet Proje ve Uygulamaları. Ankara: Bilgi Toplumu Dairesi Yayını.

Dülger, M. V. (2015). Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti. İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 1(2), 43-80.

Elattresh, J., A.M. (2022). Bilgi Güvenliği Hizmet Yönetimi: Bilgi Güvenliği Yönetimine Bir Hizmet Yönetimi Yaklaşımı Ve Bir Kurumun Müşterinin Memnuniyeti Ve Güvenirliği Üzerindeki Etkisi. Yayınlanmamış Doktora Tezi. Kastamonu Üniversitesi Fen Bilimleri Enstitüsü Malzeme Bilimi Ve Mühendisliği Ana Bilim

Dalı.

ELFANET, (2024). Stuxnet Nedir?. https://elfanet.com.tr/tr/main/article/stuxnet-nedir/105. Access date: 06/04/2024.

European Union, (2005). Patient Safety- Making It Happen Luxemburg Decleration on Patient Safety, S.1

Galetsi, P., Katsaliaki, K., & Kumar, S. (2020). Big data analytics in health sector: Theoretical framework, techniques and prospects. International Journal of Information Management, 50, 206-216.

Ganai, P. T., Bag, A., Sable, A., Abdullah, K. H., Bhatia, S., & Pant, B. (2022, April). A Detailed Investigation of Implementation of Internet of Things (IOT) in Cyber Security in Healthcare Sector. In 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 1571-1575). 28-29 April 2022 Greater Noida, India.

Gellerstedt, M. (2016). The Digitalization of Health Care Paves The Way for Improved Quality of Life. Journal of Systemics, Cybernetics and Informatics, 14, 1-10.

Gerçeker, B. (2012). Sağlık Kuruluşlarında Örgüt İklimi Ve Bilgi Güvenliğinin İlişkisi. Dokuz Eylül Üniversitesi Sağlık Bilimleri Enstitüsü Sağlıkta Kalite Geliştirme ve Akreditasyon Ana Bilim Dalı. İzmir.

Getoppos, (2024). Cyber Attack in Hospitals: Biggest Healthcare Industry Cyber Threats. https://getoppos.com/cyber-attacks-in-hospitals/. Access date: 06/04/2024.

Gopal, G., Suter-Crazzolara, C., Toldo, L., & Eberhardt, W. (2019). Digital Transformation in Healthcare–Architectures of Present and Future Information Technologies. Clinical Chemistry and Laboratory Medicine, 57(3), 328-335.S.329

Goutam, R. K. (2015). Importance of Cyber Security. International Journal of Computer Applications, 111(7), 14-15

Gritzalis, D. A. (1998). Enhancing security and improving interoperability in healthcare information systems. Medical Informatics, 23(4), 309-323.

Häyrinen, K., Saranto, K., & Nykänen, P. (2008). Definition, structure, content, use and impacts of electronic health records: a review of the research literature. International journal of medical informatics, 77(5), 291-304.

Henkoğlu, T., & Yılmaz, B. (2013). Avrupa Birliği AB Bilgi Güvenliği Politikaları. Türk Kütüphaneciliği, 27(3), 451-471.

Herland, M., Khoshgoftaar, T. M., & Wald, R. (2014). A Review of Data Mining Using Big Data in Health Informatics. Journal of Big Data, 1(1), 1-35.

Herrmann, M., Boehme, P., Mondritzki, T., Ehlers, J. P., Kavadias, S., & Truebel, H. (2018). Digital transformation and disruption of the health care sector: Internet-based observational study. Journal of medical internet research, 20(3), e104.

Huang, D. L., Rau, P. L. P., & Salvendy, G. (2010). Perception of Information Security. Behaviour & Information Technology, 29(3), 221-232.

Iqbal, M. H., Aydin, A., Brunckhorst, O., Dasgupta, P., & Ahmed, K. (2016). A Review of Wearable Technology in Medicine. Journal of The Royal Society of Medicine, 109(10), 372-380.

Iyanna, S., Kaur, P., Ractham, P., Talwar, S., & Islam, A. N. (2022). Digital transformation of healthcare sector. What is impeding adoption and continued usage of technology-driven innovations by end-users?. Journal of Business Research, 153, 150-161.

İzgi, M. C. (2014). Mahremiyet Kavramı Bağlamında Kişisel Sağlık Verileri. Türkiye Biyoetik Dergisi, 1(1), 201425-201437.

Jee, K., & Kim, G. H. (2013). Potentiality of big data in the medical sector: focus on how to reshape the healthcare system. Healthcare informatics research, 19(2), 79-85.

Kaspersky, (2024). WannaCry fidye yazılımı nedir? https://www.kaspersky.com.tr/resource-center/threats/ransomware-wannacry. Access date: 06/04/2024.

Khan, B., Fatima, H., Qureshi, A., Kumar, S., Hanan, A., Hussain, J., & Abdullah, S. (2023). Drawbacks of artificial intelligence and their potential solutions in the healthcare sector. Biomedical Materials & Devices, 1(2), 731-738.

Kissi, J., Dai, B., Owusu-Marfo, J., Bediako, I. A., Antwi, M. O., & Akey, B. C. A. (2018). A Review of Information Security Policies and Procedures for Healthcare Services. Canadian Journal of Applied Science and Technology, 6(2), 812-819.

Korkmaz, A. Ç. (2018). Geçmişten Günümüze Hasta Güvenliği. İnönü Üniversitesi Sağlık Hizmetleri Meslek Yüksek Okulu Dergisi, 6(1), 10-19.

Küzeci, E. (2019). Kişisel verilerin korunması. Ankara: Seçkin Yayıncılık.

Lindgren, I., & Jansson, G. (2013). Electronic services in the public sector: A conceptual framework. Government Information Quarterly, 30(2), 163-172.

Marttin, V., & Pehlivan, İ. (2010). ISO 27001: 2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir İnceleme. Mühendislik Bilimleri ve Tasarım Dergisi, 1(1), 49-56.

Mevzuat Bilgi Sistemi, (2016). Kişisel Verilerin Korunması Kanunu. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5. Access date:01/03/2024.

Mukherjee, S., Chittipaka, V., Baral, M. M., Pal, S. K., & Rana, S. (2022). Impact of artificial intelligence in the healthcare sector. Artificial Intelligence and Industry 4.0, 23-54.

Öğütçü, G., Köybaşı, N. A. G., & Cula, S. (2011). Elektronik Sağlık Kayıtlarının İçeriği, Hassasiyeti ve Erişim Kontrollerine Yönelik Farkındalık ve Beklentilerin Değerlendirilmesi. VIII. Ulusal Tıp Bilişimi Kongresi,

Tıp Bilişimi 2011. pp.88-97. 17-20 Kasım 2011, Xanadu Hotel, Belek, Antalya, Turkiye.

Özek, Ç. (1999). Düşünce Özgürlüğünden Bilgilenme Hakkına. İstanbul: AlfaYayınları.

Öztürk, H., Yüksek, C., & Aslan, M. (2014). Sağlık Bakanlığı Bilgi Güvenliği Politikaları Klavuzu, 2014. https://bilgiguvenligi.saglik.gov.tr/files/BilgiGüvenliğiPolitikalarıKılavuzu.pdf. Access date: 06/04/2024.

Par, Ö.E. & Soysal, E. (2011). Kişisel Sağlık Bilgilerinin Güvenliği Açısından Medula'da Kullanılan Yasa ve Standartların HIPAA ile Karşılaştırılması. VIII. Ulusal Tıp Bilişimi Kongresi, Tıp Bilişimi 2011. pp.82-87. 17-20 Kasım 2011, Xanadu Hotel, Belek, Antalya, Turkiye.

Pawar, J., Kulkarni, D., & Dhanwate, V. (2024). Understanding Cyber Security In Health Sector. Journal of Advanced Zoology, 45, 55-64.

Perednia, D. A., & Allen, A. (1995). Telemedicine Technology and Clinical Applications. JAMA, 273(6), 483-488.

Preis, B., & Susskind, L. (2022). Municipal Cybersecurity: More Work Needs to Be Done. Urban Affairs Review, 58(2), 614-629. https://doi.org/10.1177/1078087420973760

Ravì, D., Wong, C., Deligianni, F., Berthelot, M., Andreu-Perez, J., Lo, B., & Yang, G. Z. (2016). Deep learning for health informatics. IEEE journal of biomedical and health informatics, 21(1), 4-21.

Rosacker, K. M., & Olson, D. L. (2008). Public sector information system critical success factors. Transforming Government: People, Process and Policy, 2(1), 60-70.

Sağlık Bakanlığı, (2003). Sağlıkta Dönüşüm, Ankara: Türkiye Cumhuriyeti Sağlık Bakanlığı.

Sağlık Bakanlığı, (2004). Türkiye Sağlık Bilgi Sistemi Eylem Planı. Bilgi İşlem Dairesi Başkanlığı. Ankara: Türkiye Cumhuriyeti Sağlık Bakanlığı.

Schwalbe, N., & Wahl, B. (2020). Artificial intelligence and the future of global health. The Lancet, 395(10236), 1579-1586.

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of Cyber Security. International Journal of Advanced Research in Computer and Communication Engineering, 7(11), 125-128.

Shchavinsky, Y. V., Muzhanova, T. M., Yakymenko, Y. M., & Zaporozhchenko, M. M. (2023). Application Of Artificial Intelligence For Improving Situational Training Of Cybersecurity Specialists. Information Technologies and Learning Tools,97(5), 215-226.

Smith, E., & Eloff, J. H. (1999). Security in health-care information systems—current trends. International journal of medical informatics, 54(1), 39-54.

Smith, E., & Eloff, J. H. (1999). Security in health-care information systems—current trends. International journal of medical informatics, 54(1), 39-54.

Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information Security Policies in The UK Healthcare Sector: A

Critical Evaluation. Information Systems Journal, 22(1), 77-94.

Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information security policies in the UK healthcare sector: a critical evaluation. Information systems journal, 22(1), 77-94.

Tibodeau, P. (2014). Cyberattacks Could Paralyze US, Former Defence Chief Warns. https://www.computerworld.com/article/1612081/cyberattacks-could-paralyze-u-s-former-defense-chief-warns.html. Access date: 06/04/2024.

Trend Micro, (2024). RYUK fidye yazılımı nedir? https://www.trendmicro.com/tr_tr/what-is/ransomware/ryuk-ransomware.html. Access date: 06/04/2024.

Upguard, (2024). 14 Biggest Healthcare Data Breaches. https://www.upguard.com/blog/biggest-data-breaches-in-healthcare. Access date: 06/04/2024.

Uysal, B., & Yorulmaz, M. (2018). Sağlıkta Kalite Standartları ve Bilişsel Mahremiyet. Selçuk Üniversitesi Sosyal ve Teknik Araştırmalar Dergisi, (16), 24-33.

Van Deursen, N., Buchanan, W. J., & Duff, A. (2013). Monitoring information security risks within health care. Computers & Security, 37, 31-45.

Vural, Y., & Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartlari Üzerine Bir İnceleme. Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 23(2),507-522.

Yılmaz, D., Özkoç, E. E., & Öğütçü, G. (2021). Elektronik Sağlık Kayıtlarında Farkındalık. Hacettepe Sağlık İdaresi Dergisi, 24(4), 777-792.