Prof. János Besenyő PhD
Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Hungary.
Centre for Military Studies (CEMIS), Faculty of Military Science of Stellenbosch University, Republic of South Africa.
E-mail: besenyo.janos@gmail.com

Attila Máté Kovács, Research Fellow
Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Hungary
E-mail: attila.kovacs@cyber.services

DOI: 10.37458/ssj.4.1.6
Review Paper
Received: February 24, 2022
Accepted: March 19, 2023

HEALTHCARE CYBERSECURITY THREAT CONTEXT AND MITIGATION OPPORTUNITIES

Abstract: *With the rapid increase in cybersecurity incidents around the globe, no business or industry is hidden from cybercriminals' crosshairs. Cyber-attacks are evolving and becoming more complex each day, causing much damage to different financial and reputational sectors.*
The health sector (including healthcare technology) is increasingly digitized and continues to offer life-critical services. It continues to improve diagnosis, treatment, and patient care with state-of-the-art technologies. However, cybercriminals continue to exploit vulnerabilities and exfiltrate confidential patient data and other confidential information. The health care sector offers cybercriminals a rich source of confidential data and is very easy to exploit as the defense and security controls are weak. Because of the growing number of threats associated with the health sector, it is essential to understand how health care practitioners - along with concerned critical Information Technology (IT) teams - can take steps to improve the cybersecurity posture of this industry and help reduce the attack surface.
Hence, this paper discusses a critical approach to analyze the current cybersecurity challenges faced by the health care sector and relevant mitigation and other scholarly articles and research papers.

Keywords: *Health Sector, Ransomware, Cybersecurity Threats, Mitigation, Vulnerabilities*

Introduction

Events involving cybersecurity may have a substantial influence on the health sector, which includes hospitals, clinics and other healthcare organizations.

The global healthcare industry continues to undergo significant changes. Hathaliya and Tanwar (2020) point to the healthcare sector's transition from a more doctor-centric system to a technology-centric one. The increasing incorporation of state-of-the-art technologies in the healthcare sector brings more efficient and effective ways that bring precisions in medical services. However, there is a need for more developments in terms of response to cyber risks (Besenyő, Krisztina Márton, & Ryan Shaffer, 2021). Maintaining patient data privacy remains critical to ensure the preservation of data integrity.

It is necessary for healthcare firms to implement preventative measures to avoid, recognize, and respond to challenges related to cybersecurity. This may entail developing efficient defenses against cybercrime, doing periodic risk assessments and providing employees with ongoing training in cybersecurity.

Overview of the Impact of Cybersecurity Incidents on the Health Sector

A. Data & Privacy Breaches

Numerous personal and medical records held by healthcare firms are useful to hackers. Since ‘data is the new oil’ details such as social security numbers, medical histories and insurance information are of very high value specially on the black market **(Swasey 2020)**. Patients may become victims of identity theft, fraud, and other financial crimes because of the loss of this data. Additionally, it can harm healthcare companies' reputations and result in legal consequences for neglecting to secure patient data.

B. Interruptions in Critical Medical Services

The disruption of vital medical services might occur because of cyberattacks on healthcare organizations. A ransomware attack on a hospital's computer system, for instance, might make it impossible for medical staff to access patient information and deliver essential care. It

occasionally even leads to the postponement of operations and other medical procedures, endangering the lives of the patients. Healthcare companies may incur costly downtime as they attempt to resume normal operations because of service interruption.

C. Medical Data with Compromised Integrity and Confidentiality

Cybersecurity events can potentially jeopardize the integrity and confidentiality of medical data. Sensitive information, including patient diagnoses, treatments and test results, may be exposed as a result. Patients who may experience stigma or prejudice due to the information being disclosed may suffer terrible consequences due to the confidentiality breach. Additionally, there is a chance that the authenticity and quality of medical data may be impacted, which might hurt patient treatment.

D. Financial Losses

Incidents with cyber security in the healthcare industry may cause large financial losses. In addition to paying patients for the loss of their personal and medical data, the cost of the investigation and correction of the occurrence may be high. Healthcare institutions that breach patient privacy and medical information may also be subject to legal repercussions, including fines and compensation claims.

Cybersecurity Risks & Attacks associated with the health care sector

Several cybersecurity-related issues plague the healthcare sector. These issues range from malware that jeopardizes system security and patient privacy to distributed denial of service (DDoS) attacks that limit hospitals' ability to provide patient care (Saheed & Arowolo, 2021).

Although other crucial infrastructure sectors are vulnerable to cyber-attacks, the target of the healthcare industry poses unique challenges. Beyond financial damage and privacy concerns, cyberattacks may have an impact on the healthcare sector. Ransomware is a very common type of malware for hospitals since losing patient data might endanger lives. A growing concern in recent years has been the condition of cybersecurity in the healthcare sector as a result of the rise in cyber threats directed against the sector. The healthcare business is particularly vulnerable to

cyberattacks because of the confidential nature of the data it contains, the significance of its services and the widespread usage of digital technologies.

Healthcare businesses are a desirable target for cybercriminals because they hold and handle a significant volume of personal and medical information. Attacks using ransomware, which can disrupt operations widely and endanger patient safety and data security, have increased in this industry. Additionally, because they have permission to access sensitive data and systems, insider threats, such as workers and contractors, constitute a serious risk to healthcare businesses.

Issues faced in the healthcare sector concerning Cybersecurity:

1. Patient Data and Privacy Protection
2. Legacy System Vulnerabilities
3. IT Challenges in the Health Sector
4. Security Breaches
5. Complex Cybersecurity/Information Security Programs

Five ways security risks can originate from within a healthcare organization:

1. Insider Threat
2. Curiosity
3. Shadow IT
4. Human Error
5. Unintentional Actions

The healthcare industry is increasingly concerned about adversarial attacks of artificial intelligence (AI) and machine learning systems. As these systems are utilized more often to enhance health outcomes and expedite processes, cybercriminals seeking to manipulate AI algorithms and damage patients and organizations are turning their attention to them. The secure exchange of information between healthcare organizations, patients, and other stakeholders is a problem in the healthcare industry. It is essential for healthcare organizations to have robust security measures in place to protect this information due to the rapid expansion of telemedicine and the use of electronic medical records, which has increased the amount of sensitive information being transmitted and stored electronically.

The following are the most common and widely used attacks that are utilized by cybercriminals. We discuss unique attacks conducted on the health sector, their impact and the disruption caused.

1. **Ransomware**

The term "ransomware" refers to a sort of malicious software that encrypts files and closes computers, rendering them unavailable and requesting a ransom for access to them. When this occurs, crucial processes used in the healthcare industry are hampered or made completely useless. As a result, hospitals are forced to employ manual processes which slows down the medical process and eventually requires a significant amount of funds that might have been used for various other improvements in the hospital. The three most common methods that ransomware infects victim computers are phishing emails with malicious attachments, the user clicking on dangerous links, and seeing malicious advertisements (malvertising).

2. **Data Breaches**

There appear to be new hospital data breaches announced every day. Patients/victims are notified of the incident through email, and then are given two years of free credit and identity monitoring.

According to the **Ponemon Institute** and **Verizon Data Breach Investigations Report**, the health sector experiences more data breaches than any other industry. But, given the Health Insurance Portability and Accountability Act's crystal-clear, legally mandated reporting standards, there may be some room for prejudice in this claim (HIPPA). The Act makes it more likely that healthcare breaches will be reported than breaches in other sectors.

3. **DDOS Attacks**

DDoS attacks, also known as distributed denial of service attacks, are widely used by hackers and cybercriminals as a strategy, technique, and process (TTP) to overwhelm a network to the point where it is no longer usable. This can be a serious concern for healthcare workers who rely on a network connection to offer effective patient care or on Internet access to send and receive emails, prescriptions, records and other types of information. Despite this, some distributed denial of service attacks are either opportunistic or even accidental. There are several DDoS operations that target victims for social, political, ideological or economic reasons linked with a

scenario that enrages the cyber threat actors. These motives might be related to the DDoS operations themselves or to the scenario itself. Since they commonly depend on real-time communication and access to patient data, healthcare companies such as hospitals, clinics, and research centers are especially susceptible to DDoS assaults. These kinds of organizations include research facilities. For instance, a distributed denial of service (DDoS) attack on the network of a hospital can render it impossible for medical staff to access vital systems such as medical imaging systems, electronic health records, or other essential ones that are required to provide prompt and accurate patient care.

DDoS attacks can impair the security of medical data in addition to interfering with patient treatment. Hackers may try to penetrate the targeted network's security during a DDoS attack or utilize the disruption to steal sensitive data.

4. **Insider threats**

Insider threats in the healthcare industry are risks that are caused by staff members, subcontractors, or other authorized individuals who, whether knowingly or unknowingly, abuse their access to the company's information, systems, or physical assets to hurt others or commit fraud.

The sensitivity and significance of the data and assets involved, including patient health information, intellectual property, and financial information, make insider threats in the healthcare industry particularly worrisome. Insider threats may take the form of stealing patient information or other sensitive data, destroying computer systems, selling data to unauthorized parties, or participating in other fraudulent practices. Insider threats in the healthcare industry result from various reasons, including the volume of sensitive data processed, the sheer number of workers and outside contractors that have access to the data, and the complexity of the technology and systems employed by healthcare companies.

Keeping in view the impacts of Cybersecurity incidents there arises a question that “Why is Personal Health Information (PHI) more valuable than Personally Identifiable Information (PII)?”

Data breaches frequently occur in the healthcare industry. There are various reasons behind this including malware which steals confidential information, an insider intentionally or unintentionally disclosing patient information, or misplaced laptops, hard drives or USB.

On the black market, Personal Health Information (PHI) is more valuable than credit card information or standard Personally Identifiable Information (PII). Cybercriminals have a greater motivation to attack medical databases and any information related to patients. The PHI might be used or sold for their financial gains, scams, identity theft etc. According to PHI's health and human services breach report, approximately 15 million health records had been compromised.

Cybersecurity Attacks/Incidents in the Health Sector

There has been a significant increase in cybersecurity incidents and data breaches over the past few years (Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Below are the top ten data breaches (**Table 1**.) that are under investigation by the Office of Civil Rights (U.S. Department of Health & Human Services, 2020 data, see references). The victim organizations are arranged in the order of most individuals affected by the data breach.

Table 1. Top 10 Data breaches Under Investigation

No	Health Care Provider	State	Affected Persons	Breach Date	Nature of Breach
1	Regal Medical Group,	CA	3300638	Feb, 2023	Hacking
2	Lincare Holdings Inc.	FL	1737775	Oct, 2021	Hacking
3	Baptist Medical Center	TX	1608549	July, 2022	Hacking
4	Eskenazi Health	IN	1515918	Oct, 2022	Hacking
5	Community Health Network, Inc. as an Affiliated Covered Entity	IN	1500000	Nov, 2022	Breach of Confidentiality
6	The Kroger Co.	OH	1474284	Feb, 2021	Hacking
7	St. Joseph's/Candler Health System, Inc.	GA	1400000	Aug, 2021	Hacking
8	North Broward Hospital District	FL	1351431	Jan, 2022	Hacking
9	University Medical Center Southern Nevada	NV	1300000	Aug. 2021	Hacking
10	Texas Tech University Health Sciences Center	TX	1290104	July, 2022	Hacking

We pick some of the most devastating cyberattacks caused by the most common attacks utilized by cybercriminals. These are important to discuss since effective strategies and policies will be utilized to counter these attacks.

Common Spirit Health Ransomware Attack

The hack targeted Common Spirit Health (Common Spirit Notice of Data Security Incident), a major healthcare organization with 142 hospitals and over 700 care locations operating in 21 states.

How it happened?

Between September 16 and October 3, 2022, threat actors acquired access to some of the Common Spirit Health network, which was then subject to the ransomware attack. The adversary had access to some files, including files that included personal information about patients and their families at that period. When the attack was discovered, Common Spirit acted swiftly to defend its systems, control the situation, launch an investigation and ensure continuity of care. Additionally, they alerted police enforcement and they are assisting with their continuing investigation.

Impact of Common Spirit Health Ransomware Attack

In numerous regions, the attack delayed patient treatment and disrupted access to electronic health information. Over 620,000 patients' personal information, including names, addresses, phone numbers, dates of birth, and ID numbers used by the company internally, were disclosed. The attackers, however, were unable to get insurance IDs or medical record numbers.

Damage or Loss Occurred

Over 620,000 patients' sensitive personal information was made public as a result of the hack. Patients may be harmed and lose faith in the healthcare system if access to electronic health information is interrupted and patient care is delayed. Costs associated with addressing the attack and putting new security measures in place to stop such events in the future might also be high.

According to Brett Callow, threat analyst at Emsisoft, 61 hospitals operated by 61 U.S. health systems have been affected by the ransomware so far in 2022. Sensitive data, including private health information, was compromised in at least 12 of these occurrences.

Shields Health Data Security Incident

Shields Health Care Group, Inc. ("Shields") was hit by a data breach. As per initial investigation some malicious activities on the hospital network was detected. Shields offers management and imaging services. Approximately 2 million people were affected by this incident as per the (Notice of Data Security Incident - Shields Health).

What Happened?

Shields received notification of some malicious activity on March 28, 2022, which could have entailed a data breach. Shields started looking into the intrusion and collaborated with experts in the field to understand the entire nature and extent of the incident.

The investigation found that between March 7, 2022, and March 21, 2022, an unidentified actor obtained access to several Shields systems. The examination also showed that the mystery perpetrator had collected certain data during that period. Shields had discovered and investigated a security warning on or about March 18, 2022

Impact & Damage Caused

The unidentified perpetrator obtained some material while gaining unauthorized access to Shields' networks. Social Security numbers, Names, Birth dates, Home / Work address, diagnosis, billing information, insurance number and information, medical record number, patient ID, and other medical or treatment information that were impacted. Shields' management and imaging services for a subset of Facilities Partners' patients were also affected.

Advocate Aurora Health

Advocate Aurora Health is one of the largest healthcare organizations in the Midwest, operating 26 hospitals in Wisconsin and Illinois. According to data breach notification on their website they exposed the data of 3 million patients in July 2022 as a result of inappropriate usage of a widely used website tracking device.

What Happened?

Advocate Aurora Health disclosed a data breach to its patients that resulted in the exposure of the personal information of three million patients of a 26-hospital healthcare organization in Wisconsin and Illinois.. On Advocate Aurora Health's websites, where patients may log in and provide sensitive medical and personal information, Meta Pixel was improperly used, which led to the data leaking.

Impact & Damage Caused

The following patient information was exposed in the data breach:

- Dates, times and schedule of appointment
- IP address
- Proximity to an Advocate Aurora Health location
- Health Care provider information
- Diagnosis / Procedure.

Advocate Aurora Health patients have launched a class action lawsuit against the healthcare organization, demanding more than $5 million in damages.

Cybersecurity and Privacy Standards Applied in the Health Sector

Overview

The healthcare industry follows several cybersecurity guidelines, including:

- Regulations under the Health Insurance Portability and Accountability Act (HIPAA) set requirements for the confidentiality and security of protected health information (PHI) in the US. Healthcare organizations are required under HIPAA to put in place administrative, physical, and technological measures to protect the privacy, availability, and integrity of PHI (***Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC***).
- The National Institute of Standards and Technology (NIST) offers a cybersecurity framework that details policies, benchmarks and best practices for protecting information systems in the US. For healthcare businesses, the NIST framework offers a risk-based approach to cybersecurity (***Health Information Technology (IT)***.
- The International Organization for Standardization (ISO) offers several cybersecurity standards, notably the ISO 27001 standard for information security management systems. Information security management systems may be established, put into place, kept up with, and continually improved using the framework provided by the ISO 27001 standard (***ISO 27799:2016(en) Health informatics — Information security management in health using ISO/IEC 27002***).

- The European Union Agency for Cybersecurity (ENISA) **(*Health sector*)** offers the European Union advice and recommendations on cybersecurity standards. The advice provided by ENISA addresses a variety of subjects, such as risk management, incident response, and information system security procedures.
- Payment Card Industry Data Security Standard **(PCI DSS)** A security requirement for businesses that process credit card payments are called PCI DSS. Healthcare organizations that accept payments are required to adhere to the PCI DSS standard, despite not being specifically related to healthcare.

The company's size, complexity and risk profile, as well as other considerations, determine which cybersecurity standard is the most successful for the healthcare industry. Given that it is a legal necessity, HIPAA is an important standard for healthcare firms doing business in the US. A flexible, risk-based strategy that can be customized to match the needs of healthcare organizations is offered by the NIST framework, which is also frequently employed. For larger healthcare companies with sophisticated information systems, the ISO 27001 standard offers a complete framework for information security management. Healthcare firms operating in the EU can benefit from ENISA's recommendations.

Health Insurance Portability and Accountability Act (HIPPA)

The Health Insurance Portability and Accountability Act, also known as HIPAA, was passed into federal law in the US in 1996. HIPAA's primary objective is to safeguard the confidentiality and security of people's protected health information (PHI). The term "covered entities" refers to healthcare providers, health plans, and healthcare clearinghouses. The statute also covers business partners who collaborate with covered organizations and have access to PHI. The purpose of the federal statute known as HIPAA is to safeguard the confidentiality and security of personal health information. It establishes federal guidelines for the handling, sharing, and protection of PHI and grants people certain rights concerning their PHI. For covered companies to avoid potential fines and penalties and to keep the trust of their patients, compliance with HIPAA is crucial.

The Privacy Rule and the Security Rule are the two primary parts of HIPAA. The Privacy Rule controls how covered entities may use and disclose PHI. It defines nationwide guidelines for PHI's usage, accessibility, and disclosure to third parties. The Privacy Rule also grants individuals certain rights about their PHI, such as the ability to view and get a copy of their PHI, the right to update their PHI, and the right to complain if they feel their privacy rights have been infringed.

On the other side, the Security Rule establishes federal requirements for the security of electronic PHI. It mandates that covered entities take administrative, physical and technological measures to preserve the privacy, availability, and integrity of PHI. The Security Regulation also mandates that covered businesses do routine risk analyses to find possible security threats and vulnerabilities and to implement the necessary countermeasures.

From the standpoint of a healthcare provider, HIPAA compliance is crucial. To guarantee the privacy and security of PHI, they must have the proper policies, processes, and safety measures in place. This entails imparting proper access restrictions, including special user IDs and passwords, as well as educating their employees on HIPAA requirements and how to manage PHI. Also, they need to be ready to respond to HIPAA violations subject to harsh fines and penalties.

General Data Protection Regular (GDPR)

On May 25, 2018, the European Union implemented the General Data Protection Regulation (GDPR), a comprehensive and expansive data privacy policy (EU). The GDPR, which updates the 1995 Data Protection Regulation, aims to safeguard individual privacy rights, standardize data protection legislation across EU member states and improve how businesses acquire, use, and handle personal data. No matter where the firm is located, the GDPR applies to all organizations that gather or handle personal data from EU persons.

The GDPR's main requirements are as follows:

- The GDPR does extend the definition of personal data to encompass all data that may be used to identify a specific person, such as IP addresses, biometric information and social media posts.
- **Consent:** Before collecting, processing, or utilizing a person's data, businesses must receive "unambiguous" consent from the person in question. Specific, informed, voluntarily provided, and revocable permission is required.
- **Rights of the data subject**: The GDPR grants individuals the right to see, update, and delete their personal information. It also grants them the right to data portability, which enables them to move their personal information from one organization to another.
- The GDPR mandates that enterprises perform data protection impact assessments (DPIAs) to identify and reduce privacy risks related to their data processing operations.
- **Data breaches:** Under the GDPR, enterprises must notify affected persons if there is a high risk that their rights and freedoms may have been violated and disclose data breaches to the appropriate supervisory authority. Furthermore, this must happen within 72 hours of becoming aware of any incident happening to data.
- Data protection officers (DPOs): The GDPR mandates the appointment of a DPO to supervise data protection compliance in certain enterprises.
- **Accountability:** Under the GDPR, businesses must put in place the proper organizational and technical safeguards to guarantee compliance with the rules and to provide supervisory authorities with proof of that compliance.

Supervisory authorities in each EU member state are tasked with enforcing the GDPR, and they have the authority to conduct audits and impose penalties on noncompliant firms. The maximum penalty for non-compliance is €20 million, which is equal to 4% of the company's annual global revenue, whichever is larger **(Fines / Penalties - General Data Protection Regulation (GDPR))**.

Impact of regulations on healthcare cybersecurity

The creation and use of cybersecurity measures in healthcare companies are significantly impacted by laws like the GDPR and the HIPAA. These laws establish data privacy, security, and breach reporting requirements to protect sensitive personal and health information.

Healthcare organizations must create and maintain administrative, physical, and technical measures to secure the confidentiality, integrity and availability of electronically protected health information following HIPAA rules in the United States (ePHI). Healthcare firms must comply with HIPAA standards by putting in place the proper privacy and security policies, processes, and employee training to protect ePHI.

Organizations handling personal data, including healthcare data, are required to comply with the GDPR in the European Union by putting in place the necessary organizational and technical safeguards. The GDPR mandates that people have the right to view their data, ask for its deletion, and be notified when there has been a data breach.

The following analysis can be used to determine how HIPAA and GDPR have affected healthcare cybersecurity measures:

Risks related to cybersecurity are becoming more widely recognized in healthcare enterprises because of HIPAA and GDPR. They have emphasized the value of safeguarding patient information and encouraged the use of cybersecurity precautions such as encryption, access control, and network monitoring.

Installation of technological safeguards

To secure patient data, healthcare companies are required under HIPAA and GDPR to adopt technical safeguards. Firewalls, encryption and two-factor authentication are some of these security measures. Several steps have been taken by healthcare institutions to abide by rules and safeguard patient data.

Concentrate on employee education and awareness

HIPAA and GDPR mandate that healthcare firms educate and inform their staff about the value of data privacy and security. Healthcare firms have put in place awareness campaigns and training programs to make sure that their staff members are knowledgeable of the dangers of cyber-attacks and how to avoid them.

Enhanced notification requirements for data breaches

Under HIPAA and GDPR, healthcare businesses are required to notify the appropriate authorities and any impacted persons of data breaches. Because of this, healthcare companies now have policies and practices in place for breach notification.

Possibility of higher costs

For healthcare firms, complying with HIPAA and GDPR can be expensive. To guarantee compliance with the rules, they could need to make new cybersecurity investments and recruit more personnel.

Need for effective Cybersecurity strategies and policies for securing health data

Effective cybersecurity strategies and regulations are essential in today's digital healthcare environment for protecting health data. Because cyber threats and assaults are increasingly becoming more frequent, sophisticated and targeted, it is becoming more and more clear that strong cybersecurity solutions are required. A variety of negative effects, including the loss of patient privacy, financial loss, legal and regulatory implications and reputational harm, can result from cyberattacks on healthcare companies.

Protecting patient privacy is one of the most important justifications for implementing cybersecurity strategies and regulations. Sensitive information concerning a person's medical history, treatment options, and personal details are all contained in health data. Effective cybersecurity techniques and procedures are required to safeguard sensitive data from unwanted access and disclosure. Losing patient privacy can have disastrous repercussions, including harm to one's reputation, legal culpability, and loss of public trust.

Preventing data breaches is another important factor in the health sector's adoption of good cybersecurity methods and procedures. Since they keep a significant amount of sensitive data, healthcare companies are a top target for hackers. Data breaches from cyberattacks on healthcare businesses can be expensive to fix and harm a company's reputation for a long time. Effective cybersecurity strategies and policies may lessen the impact of data breaches if they do occur and assist prevent them from happening in the first place.

While adopting cybersecurity objectives and policies in the health industry, maintaining regulatory compliance is another essential factor to consider. Several laws and standards pertaining to the protection of personal information and privacy, such as the Health Insurance Portability and Accountability Act, apply to healthcare businesses (HIPAA). Maintaining regulatory compliance and avoiding fines need effective cybersecurity tactics and practices.

Effective cybersecurity methods and procedures can protect against financial losses in addition to the reasons listed above. Healthcare institutions are not exempt from the threat posed by cybercrime, which has considerable financial costs. A cyber-attack may result in financial loss, harm to one's reputation, and expensive legal fees. These losses can be prevented with the use of efficient cybersecurity tactics and procedures. Healthcare businesses should undertake a risk assessment to identify possible threats and vulnerabilities to build successful cybersecurity plans and procedures (Thamer, N., & Alubady, R. (2021, April). After that, they should put in place technological safeguards like access controls, firewalls, and encryption while also creating rules and practices for data access, usage, and storage. To inform personnel about cybersecurity risks and best practices, consistent training and awareness initiatives should be put in place.

References

1. Hathaliya, J.J. and Tanwar, S. (2020). An Exhaustive Survey on Security and Privacy Issues in Healthcare 4.0. Computer Communications, 153, pp. 311–335. doi: https://doi.org/10.1016/j.comcom.2020.02.018.
2. Besenyő, J., Krisztina Márton & Ryan Shaffer (2021) Hospital Attacks Since 9/11: An Analysis of Terrorism Targeting Healthcare Facilities and Workers, Studies in Conflict & Terrorism, DOI: 10.1080/1057610X.2021.1937821.
3. Swasey, K. (2020). Insufficient healthcare cybersecurity invites ransomware attacks and sale of phi on the dark web. Center for Anticipatory Intelligence Student Research Reports.
4. Saheed, Y. K., & Arowolo, M. O. (2021). Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms. IEEE Access, 9, 161546–161554. https://doi.org/10.1109/access.2021.3128837.
5. 2022 Data Breach Investigations Report. (2022.). Verizon Business. https://www.verizon.com/business/resources/reports/dbir/. Accessed: 2023-02-24
6. Cost of a data breach 2022. (2022). IBM - Deutschland | IBM. https://www.ibm.com/reports/data-breach. Accessed: 2023-02-24
7. Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. Business horizons, 62(4), 539-548.
8. U.S. Department of Health & Human Services - Office for Civil Rights. (accessed for 2020 data.). U.S. Department of Health & Human Services - Office for Civil Rights. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Accessed: 2023-02-24
9. Notice of Data Security Incident. (n.d.). CommonSpirit Health | Compassionate Care for Our Communities. https://www.commonspirit.org/update/notice-of-data-security-incident. Accessed: 2023-02-24
10. Notice of Data Security Incident - Shields Health. (n.d.). Shields Health. https://shields.com/notice-of-data-security-incident/. Accessed: 2023-02-24
11. Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies. (n.d.). Fierce Healthcare. https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3. Accessed: 2023-02-24
12. Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC. (1996) Centers for Disease Control and Prevention. https://www.cdc.gov/phlp/publications/topic/hipaa.html. Accessed: 2023-02-24
13. Health Information Technology (IT). (n.d.). NIST. https://www.nist.gov/healthcare. Accessed: 2023-02-24
14. ISO 27799:2016(en) Health informatics — Information security management in health using ISO/IEC 27002. (2016). Online Browsing Platform (OBP).https://www.iso.org/obp/ui/#iso:std:iso:27799:ed-2:v1:en. Accessed: 2023-02-24

15. Health sector. (2014). ENISA. https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/health. Accessed: 2023-02-24
16. Fines / Penalties - General Data Protection Regulation (GDPR). (2016.). General Data Protection Regulation (GDPR). https://gdpr-info.eu/issues/fines-penalties/#:~:text=83(4)%20GDPR%20sets%20forth,to%20that%20used%20in%20Art. Accessed: 2023-02-24
17. Thamer, N., & Alubady, R. (2021). A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research. In: 2021 1st Babylon International Conference on Information Technology and Science (BICITS) (pp. 210-216)