Journal of Artificial Intelligence General Science (JAIGS)

ISSN: 3006-4023 (Online), Volume 6 , Issue 1, 2024 DOI: 10.60087

Home page https://ojs.boulibrary.com/index.php/JAIGS

JAIGS
JOURNAL OF ARTIFICIAL INTELLIGENCE GENERAL SCIENCE
JAI GS
SHAPING TOMORROW: INNOVATIONS AND TRENDS IN ARTIFICIAL INTELLIGENCE
VOL. 5 NO. 1 (2024)

Cybersecurity Threats in Healthcare IT: Challenges, Risks, and Mitigation Strategies

Md Jawadur Rahim[1], Muhammad Ihsan Ibn Rahim[2], Ahlina Afroz[3], Omolola Akinola[4]

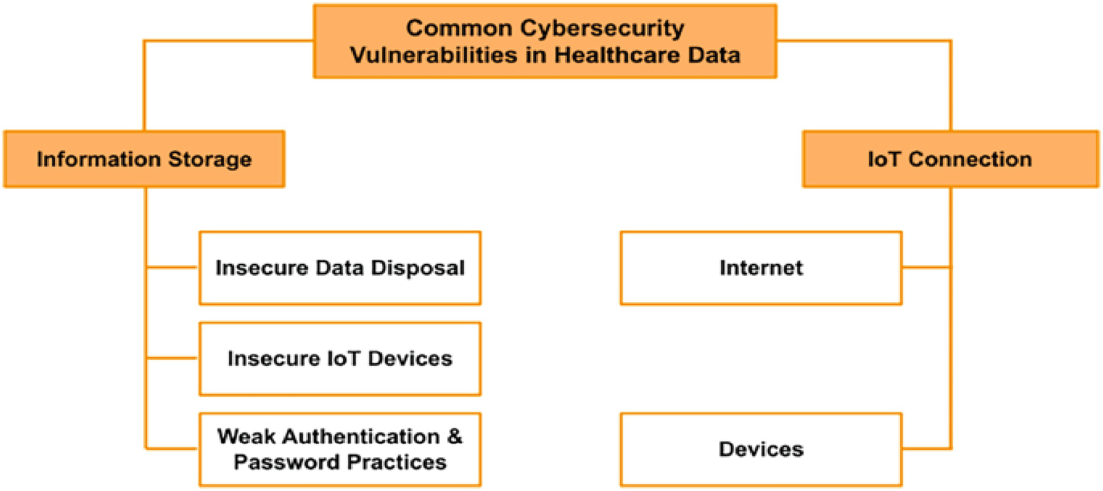
[1]HCS Home Health Care Services of NY.
[2]Graduate Teaching Assistant at University of Louisiana.
[3,4]Independent Researcher.

Abstract

The healthcare industry's reliance on digital technology to improve patient care, operations, and performance has exposed it to cybersecurity threats. The extensive capture, storage, and transmission of confidential data by healthcare institutions has led to a significant prevalence of cyber-attacks. The intersection of healthcare and information technology presents considerable challenges, with patient privacy, the security of medical devices, and the continuity of essential healthcare services all at risk. This study offers a contemporary contextual analysis of IT cybersecurity concerns within the healthcare sector. It employs a systematic methodology to delineate critical risk factors and threats, the strategies they might utilize to attain their compromise aims, and the repercussions they may impose on healthcare delivery. It also explores the measures and guidelines to address this risk. The study highlights the existence of many threats experienced by healthcare organizations, such as data theft and leakage, ransomware, cyber-attacks in different forms, and contaminated medical equipment. One prominent example is the WannaCry attack on the United Kingdom's National Health Service in 2017. According to the survey, there is a severe scarcity of qualified personnel in healthcare organizations who can defend against cyber threats effectively and efficiently, underscoring the urgent need for skilled professionals in cybersecurity. This analysis also discusses various considerations concerning achieving high availability and protecting data in healthcare businesses. It examines how emerging applications like IoMT enhance the quality of medical services for patients and the security challenges these devices pose. The report evaluates the sufficiency of existing regulatory guidelines in addressing emerging dangers, including HIPAA vulnerabilities. The current definitive framework underscores the critical importance of enhancing cybersecurity within healthcare IT. It elucidates optimal strategies for mitigating cyber hazards by promoting technological prevention, staff training, and adherence to organizational policies. The work emphasizes the necessity for ongoing research, the establishment of collaboration between medical professionals and IT security experts, and the formulation of effective strategies to protect patient information and ensure the continuity of healthcare delivery in the face of increasing cyber-attack threats in digitalization.

Keywords:
Cybersecurity, Healthcare IT, Data breaches, Ransomware, Electronic Health Records (EHRs), Internet of Medical Things (IoMT), multi-factor authentication, Telemedicine, Artificial Intelligence in cybersecurity, Cyber-attack vectors, Healthcare data analytics.

***ARTICLE INFO:** Received: 19.10.2024 Accepted: 10.11.2024 Published: 03.12.2024*


Common Cybersecurity Vulnerabilities in Healthcare Data
Information Storage
IoT Connection
Insecure Data Disposal
Insecure IoT Devices
Weak Authentication & Password Practices
Internet
Devices

INTRODUCTION AND BACKGROUND

Introduction

Through information technology, the healthcare industry has experienced a dramatic digital change in the past several years, improving efficiency, streamlined operations, and patient care. Internet of Medical Things (IoMT) devices, telemedicine platforms, and electronic health records (EHRs) are essential to contemporary healthcare. Patient information, medical equipment, and even critical healthcare services are at risk because the healthcare industry has been introduced to an astronomical number of cybersecurity threats due to its rapid expansion in the digital world. Another study conducted among healthcare executives revealed that 81% of them have shown their businesses' exposure to cyber-attacks in the last two years, and this has identified the healthcare industry as a favorite haven for cyber criminals (KPMG, 2015). As the figure indicates, it is high time to improve the understanding of cybersecurity in healthcare IT.

Cyber threats affect healthcare more than other industries because they are highly specialized. Kruse et al. (2017) argued that most healthcare companies possess and store substantive personal information, finances, and health records. The amount and type of information that healthcare databases store make it possible for hackers who seek vulnerabilities in information systems to consider the healthcare databases utterly irresistible. Furthermore, because the service provided is consistently critical for patients' lives, cyberattack disruptions are detrimental to human life. It is thus agreed that a hospital's medical equipment and network create complexity; based on this argument by Martin et al. (2017), they determine patient safety and care delivery to be highly susceptible to the impact of an SPOF.

Cybersecurity threats in healthcare IT encompass various attack vectors and constantly evolving criminal activities. The three top undesirable risks affecting healthcare businesses are data theft, ransomware assaults, and tampering with medical equipment. One potential peril of such risks is the WannaCry ransomware attack in 2017 on the UK's National Health Service (NHS). The National Audit Office (2017) reported that this assault led to the cancellation of thousands of appointments and operations, highlighting the potential disruption cyber disasters can cause in healthcare environments. Protecting sensitive information and vital infrastructure is already a daunting task, and it is made even more so because cyber-attacks are becoming more sophisticated, and healthcare organizations continue to face a severe shortage of cybersecurity professionals (Landi, 2015).

In light of these increasing dangers, the regulatory environment for healthcare cybersecurity has also changed. The United States has established the Health Insurance Portability and Accountability Act (HIPAA) to safeguard private patient information. However, Shenoy and Appel (2017) noted that regulatory frameworks are not always up to dealing with new and emerging dangers because technology advances at such a dizzying rate. Healthcare firms have even more significant challenges in this regard, linked to fluctuating regulatory demands and new technologies that simultaneously make it challenging to guarantee robust protection against cyber threats and compliance. Inter-country cooperation and working under international standards is essential given that cyber threats are often cross-border or Transnational, making the task even more challenging.

As the healthcare sector becomes more dependent on technology and data, it is crucial to be highly alert against cyber threats to protect patients and uphold trust in clinical practices. This review aims to synthesize existing literature to discuss the current status of cybersecurity threats in Health IT and highlight the potential implications of these threats. By identifying these implications, we can better understand the gravity of the situation and work towards reducing such risks. This review seeks to expand the existing literature on healthcare information system security and the resilience of critical healthcare services to emerging cybersecurity threats with the results gleaned from the analyses of peer-reviewed and grey literature and case studies conducted in other health facilities. By sharing the information presented in this assessment with healthcare practitioners, policymakers, and technology vendors, the authors aim to foster a collective effort to enhance healthcare cybersecurity.

Background of Cybersecurity Threats in Healthcare IT

1) 1.2.1 Evolution of Healthcare IT and Associated Cybersecurity Challenges

The use of information technology in the healthcare sector has received a significant boost in the past two decades. This shift has occurred due to the need to increase the impact of patient care, enhance operation capacity, and reduce costs. According to Dimitrov (2016), using EHRs has been pivotal in strengthening the digital trend of new health records as they assist healthcare providers in storing, retrieving, and sharing patient information. Digitization has also led to new risks in susceptibility to cyber-attacks. Williams and Woodward (2015) noted that the change from paper means to electronic solutions has only made the data even more prone to hackers.

The use of interlinked healthcare technologies and the IoMT has further complicated the security questions in healthcare. According to Burns et al. (2016), the reliance in modern healthcare on connected devices, including diagnostic, delivery, and monitoring tools like infusion pumps and implantable cardiac defibrillators, creates new cyber risks. These gadgets often run on outdated software or lack stringent security features and can be exploited to gain unlawful access to a hospital's network or even manipulate patient care. Parmar (2012), for instance, pointed out that insulin pumps for people with diabetes are easily hacked and, therefore, shows that risks associated with these IoT medical devices are inherent.

On the other hand, mobile health and telemedicine are new areas with new cybersecurity challenges. According to Kotz et al. (2016), using the PHS to transfer health information using potentially inconvenient networks amplifies the risk of interception and uncontrolled access. Furthermore, citing personnel-owned portable gadgets in aggravating patient information compromises security since it uses such gadgets to retrieve such information, which adds worry over information leakage and shame and mortification over lost or stolen gadgets. Telemedicine has been forwarded due to the COVID-19 outbreak, and according to Hackett (2020), there has been a significant increase in cybersecurity attacks on healthcare professionals during this virus outbreak.

Surgical retrieval results show that healthcare institutions become more insecure due to integrating more connected solutions as they search for better interconnectivity and data exchange. Walker (2017) notes that while interoperability standards help the healthcare industries accomplish their mission of creating better quality patient care, the matter simultaneously challenges the security of health information across many systems and institutions. The issue is managing connectivity requirements to facilitate data transfer and the challenges of implementing secure systems for PATIENTS' privacy and protection of health care information systems.

1.2.2Types and Impacts of Cybersecurity Threats in Healthcare

Cybersecurity threats are diverse in the healthcare industry, and the impact of these threats could be devastating to both patients and healthcare organizations. Some of the most frequent risks include data breaches, which is quite concerning. IBM's Data Breach Calculator (n.d.) shows that the healthcare industry remains at the top as the costliest regarding the average cost per data breach. These breaches can lead to leakage of essential patient data, identity thefts, and fraud, and endangering the reputation of the concerned healthcare facilities. The cyber-attack on the 2015 Anthem health insurance, stated by Abelson and Goldstein (2015), provides an understanding of the potential size of the cyber threats in the health sector wherein the personal information of up to 80 million individuals was compromised.

Today, it is possible to talk about ransomware attacks as a hazardous cyber threat in healthcare. These assaults ensure that an organization's data is locked or held and that a ransom is paid before the data is released. In particular, the WannaCry ransomware attack on the UK's National Health Service (NHS) in 2017, which Deane-McKenna (2017) vividly described, disrupted thousands of consultations and operations, which point to the fact of severe consequences of the cyber terrorists' actions for patient outcomes. Healthcare has become one of the most vulnerable sectors to ransomware attacks as it strives to get the money needed to restore essential systems as soon as possible.

This type of threat constitutes a significant risk to healthcare companies, but it is not given much attention compared to outside threats. As highlighted by Arndt (2018), insider threats, whereby the actors may act intentionally or inadvertently, are partly blamed for contributing to data breaches in the healthcare sector. Insider threats may involve individuals seeking to gain information such as health records or disgruntled employees intent on divulging privileged information. The problem of risk management of insiders is intensified with the need for medical workers to have unrestricted access to patients' records to address their needs promptly.

The hacking of medical devices is a unique and potentially lethal cybersecurity threat in healthcare. Wireless attacks have been shown to place implantable cardiac defibrillators at risk. According to Halperin et al. (2008), this poses a significant concern about the likelihood of malign actors controlling the devices. Further, Pycroft et al. (2016) examined the potential risk of "Brain Jacking," where deep stimulation devices might be vulnerable to cyber exploitation. The described situations prove that cybersecurity threats are not only a problem that can affect any business and organization but an issue that can lead to immediate harm to patients and lower the quality of medical care.

1.2.3Regulatory Landscape and Compliance Challenges

The regulation of healthcare cybersecurity is complex and dynamic due to newly developed threats and technologies in cyberspace. Concerning the protection of healthcare data in the United States, the pillar that remains supporting the laws is the HIPAA of 1996. HIPAA provided rules for the protection of ePHI, which have been adopted according to the

US Department of Health and Human Services (1996). In healthcare, new technology presents compliance problems because of the fast pace of change in technology instead of changes in compliance rules.

The HITECH Act, which came to the limelight in 2009, increased the fine for HIPAA noncompliance and enhanced the rules of the act even more. According to Health IT (n.d.), this law aimed to improve patient information protection and increase health information technology adoption. Kruse et al. (2017) further noted that such laws could be complicated and expensive for healthcare providers, especially for those firms that cannot afford adequate cybersecurity and compliance.

The US Food and Drug Administration – FDA has perceived the enhanced probability of cyber-attacks on medical equipment and has ensured that cybersecurity has become a concern in all stages of products. Leading medical equipment manufacturers can still seek recommendations on cybersecurity management in the FDA guidelines for premarket (2014) and postmarket (2016). These documents stress the importance of integrating cybersecurity at the device's conception and continuously protecting and securing it over its lifespan. Nevertheless, Storm (2015) suggests that even secure consumer electronics products may eventually be vulnerable to cyber risks if these risks are continuously escalating.

The General Data Protection Regulation of the European Union and other international regulations have also played a pivotal role in shaping the cybersecurity processes in healthcare facilities across the globe. The stringent regulations required by the GDPR on data protection and breach notification have pressured healthcare firms to improve their cybersecurity stance and invest in better data protection systems (Armstrong, 2018). Maintaining concise but compelling cyber security while navigating the complex landscape of the multiple standards of healthcare across the world is challenging for international healthcare companies.

1.2.4Emerging Technologies and Future Cybersecurity Challenges

The fast technological advancement in the delivery of healthcare systems is providing new cybersecurity opportunities and challenges. A growing focus and potential for peril has emerged on the Internet of Medical Things or IoMT. According to Kumari et al. (2019), the present world has witnessed wearables and associated compliant health devices create an extensive network of points of cyber-attack vulnerabilities. The security of this diverse device ecosystem with heterogeneous computing power and protection mechanisms will pose significant challenges to both device manufacturers and healthcare companies.

AI and ML: Their roles are in four of the most utilized categories in healthcare: diagnostic tools, predictive analytics, clinical decision, and support tools. Such technologies do not avoid new cybersecurity threats despite the potential to improve healthcare outcomes significantly. According to Martin et al. (2017), it is common for AI systems in healthcare to rely on vast databases of patients' data, which can be seen as a privacy invasion or potential for adversarial attacks to influence the procedure of AI decision-making.

The takeoff of cloud computing in healthcare has accelerated in recent decades as this approach offers efficient and elastic ways of managing large volumes of health information. However, as Bell and Ebert (2015) note, transitioning to cloud-based systems introduces more security issues, such as data localization issues and the need for encryption and stringent access controls. All organizations involved in providing healthcare services must critically examine the security policies of cloud service providers to ensure that the companies comply with relevant rules when adopting cloud technologies.

Blockchain, a model with the potential to significantly improve healthcare data quality and ensure secure information exchange, is a crucial focus of this research. As Dimitrov (2016) suggests, blockchain could revolutionize health information exchange by providing a traceable and immutable record of data transactions through a decentralized public ledger. However, blockchain application in healthcare also raises important questions of scalability, privacy, and legal concerns that this research aims to address.

B. 1.3 Aim and Objectives

This extensive research will explore and evaluate the current status of cybersecurity threats in healthcare information technology, consider the potential consequences, and identify measures to mitigate these risks. To attain this objective, the subsequent goals have been delineated:

1. To propose an assessment and categorize the leading cyber risks that affect healthcare companies in the digital environment.
2. They are presented below to assess the impact of these threats on patient care, data privacy, and the overall functioning of healthcare systems.
3. Analyzing the performance of current legal structures and compliance requirements for eliminating cybersecurity issues in healthcare settings.
4. To examine the effects of exponential technologies in creating new cyber threats and practical solutions for addressing such threats.
5. To offer recommendations and best practices for enhancing protective activities and medical facility cybersecurity in healthcare IT environments.

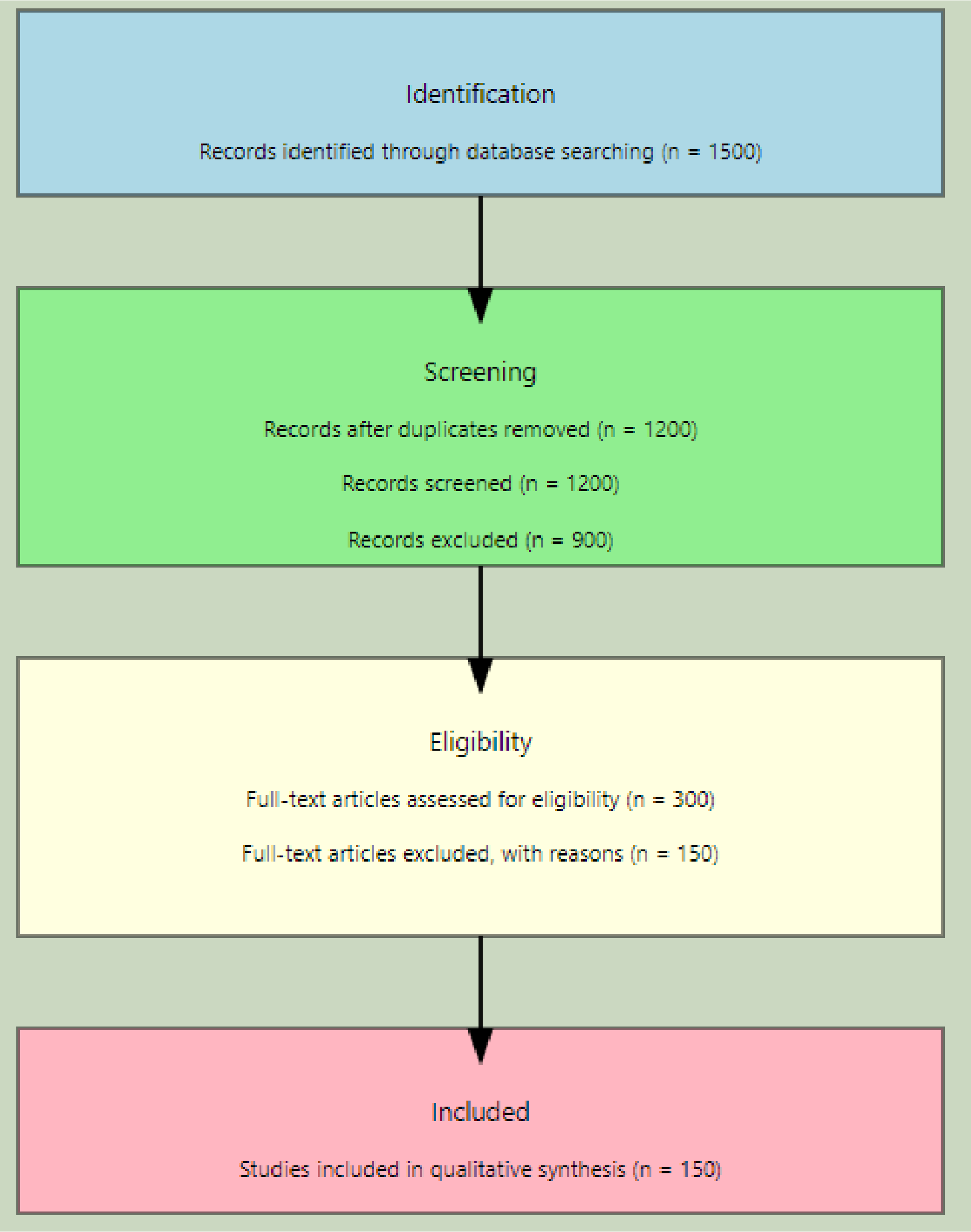
This evaluation aims to contribute to and improve the current debate for protecting hospital information systems and sustaining critical healthcare services from current and future cyber threats.

METHODOLOGY

The study was conducted to assess the risks associated with cybersecurity in Healthcare Information Systems in a structured and exhaustive manner. It followed a standard methodological process guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) tools.

An initial literature search was conducted through an electronic database search using the publishers' databases such as PUBMED, IEEE Xplore, ACM digital library, and Google Scholar. This paper focuses on the following areas by using the search terms: "Hospital Ransomware," "Hospital Cybersecurity," "Medical Data Breaches," and "IoMT Security". Moreover, OR operators were used to extend the search and include all sources.

After the database search, a two-stage selection process was adopted. In the first screening step, the two researchers evaluated the focus of the titles and abstracts of all the related articles found. Decision-making was done by compounding ideas with discussions to entail a consensus. First, the second stage involved a full-text review of the selected articles based on specific inclusion and exclusion criteria. Studies that concentrated on cybersecurity threats specific to healthcare IT, their impacts, and mitigation strategies were incorporated. In contrast, those that addressed general IT security without a healthcare context were excluded.


Identification
Records identified through database searching (n = 1500)
Screening
Records after duplicates removed (n = 1200)
Records screened (n = 1200)
Records excluded (n = 900)
Eligibility
Full-text articles assessed for eligibility (n = 300)
Full-text articles excluded, with reasons (n = 150)
Included
Studies included in qualitative synthesis (n = 150)

a) *Figure 1: PRISMA Flow Diagram for Literature Review Process*

The review also included industry papers, government publications, and credible news sources to enhance academic literature. These sources provided relevant information regarding cyber occurrences, new dangers, and standard industrial practices. Case studies of significant cybersecurity incidents in healthcare settings were carefully considered since they provided tangible illustrations of the difficulties encountered by the industry.

The data extraction process was meticulously conducted using a uniform method, ensuring consistency across all the sources. The comprehensive data focused on various cybersecurity risks, their prevalence, impact on healthcare operations, existing security measures, and suggested remedies. The synthesis and analysis of this data uncovered trends, common themes, and knowledge gaps, providing a robust foundation for our review.

To determine the quality of each study, we used the Cochrane Risk of Bias Tool for RCTs and the Newcastle-Ottawa Scale for observational studies. Qualitative data analyses followed the guidelines laid out by the Critical Appraisal Skills Program (CASP). This quality assessment facilitated weighing the strength of evidence from various sources.

The systematic approach to analyzing the collected data employed theme analysis. In doing so, we also acted upon the data we extracted, searched for patterns, and finally identified picture-level conclusions that would answer the questions posed by the review. The theme analysis was not a one-step process, but several cycles of improvement and consolidation were made during the examination.

Figure 1 illustrates the flowchart created to explain the structure of the process. This flowchart presents all the procedures for conducting research, from searching databases to synthesizing the results. It summarizes all the studies identified, assessed, and utilized in an evaluation.

During the review process, regular team meetings were held to discuss results challenges and review interpretations. This practice ensured that all team members were updated and involved in the process, thereby enhancing the validity and trustworthiness of the findings presented in the review. Finally, we summarize all the gathered data we have analyzed to answer our review questions and paint the big picture of what threats act against healthcare IT cybersecurity and potential solutions.

RESULTS FROM THE REVIEWED LITERATURE SOURCES

Major Cybersecurity in the Healthcare Industry

Attacks Assaults on Connected Medical Devices: There is a significant vulnerability in healthcare cybersecurity due to connected medical devices. According to Williams and Woodward (2015), these devices often run using outdated operating systems or do not have sufficiently sophisticated security systems, which makes them irresistible to hackers. Consequently, hackers are capable of fiddling with insulin pumps and cardiac implants to endanger patient's security, as suggested by Halperin and his counterparts (Halperin et al., 2008; Pycroft et al., 2016). As IoMT devices become more integrated into the clinical setting, the attack surface expands for several reasons. Kumari et al. (2019) conclude that each attached device could represent an avenue for adversarial intent.

Email: Email phishing represents a current threat to healthcare organizations' security. According to Kruse et al. (2017), cybercriminals often attack healthcare workers using human weaknesses to gain illegitimate access to information. Such attacks may lead to the leakage of vital information and identity theft or be used to support more complicated cyber incidents. The healthcare industry, which widely uses email for patient care collaboration and general communication, is highly exposed to phishing attempts. One way to control this risk is to train personnel to recognize and respond to attempts at phishing (Martin et al., 2017).

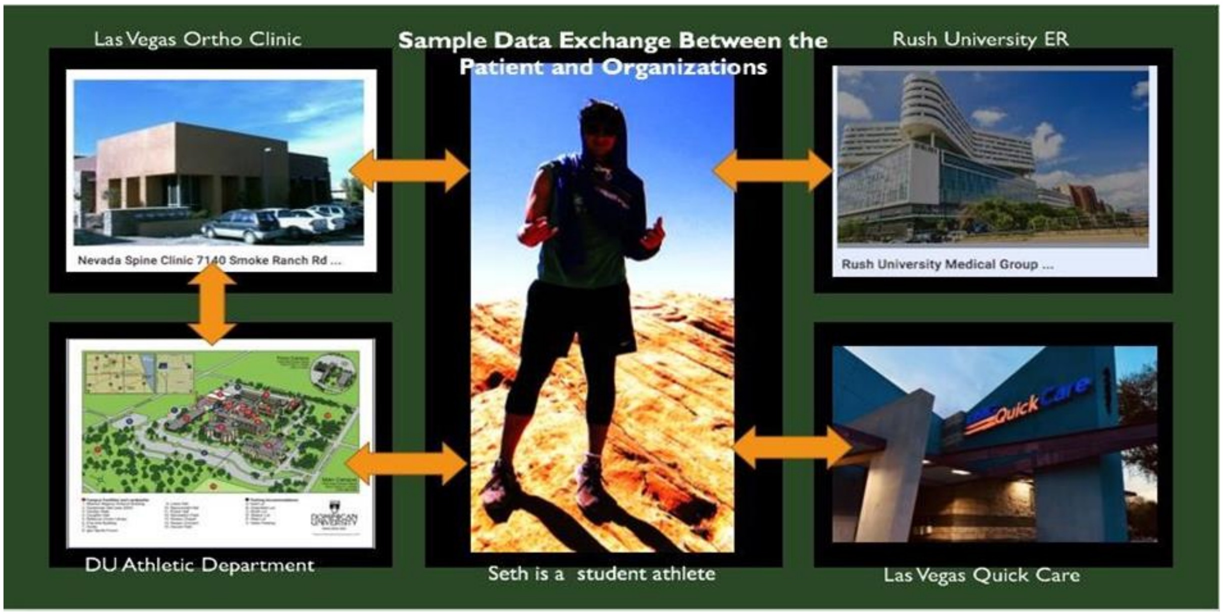
Ransomware: Ransomware attacks remain among the major threats facing healthcare organizations, and the results of their attacks can be critically devastating to patient care and the preservation of data. Among recent cyber-attacks, one can mention the 2017 WannaCry ransomware attack on facilities of the UK's National Health Service to indicate the kind of consequences that such acts can bring to healthcare management (National Audit Office, 2017). Patient records, for example, could be locked and denied to both patient and doctor, leading to interference with medical delivery. The nature of the health care services creates high pressure, forcing enterprises to give in to the ransom demands, thus making them attractive targets to hackers. Full-scale backup regimes and post-incident response plans should be implemented to mitigate the impact of ransomware attacks (Burns et al., 2016).

Loss or Theft of Equipment or Data: Healthcare cybersecurity suffers significantly from the loss or theft of equipment containing pertinent patient data. Pagers, cell phones, laptop computers, and flash drives used by healthcare people can easily be lost or stolen, so they can potentially jeopardize voluminous patient data. Kotz et al. (2016) argue that for adequate security, strong encryption should be used to protect data on the devices, while remote wipes should be available on all the devices containing patient information. In addition, protection measures dealing with the utilization and transportation of devices containing sensitive information are necessary to reduce the predictive leakage of information resulting from the loss or theft of the device.

Insider, Accidental, or Intentional Data Loss: There is always a considerable risk of insider threats, whether accidental or intentional, they pose a high risk to healthcare data security. Unintentional or deliberate loss of sensitive information is possible when staff with legal privilege to access patient details compromise the data, say Shenoy and Appel (2017). Most data losses are likely to occur accidentally, for example, through email send-outs to the wrong recipients or mistaking the rights of a database. Motive-driven: Dissatisfied employees or people with ill intentions to get financial benefits pose high risks of data theft. Strict access control measures, regular security sensitization, and monitoring devices to identify insiders accessing information abnormally are vital ways of mitigating insider threats in healthcare organizations (Kruse et al., 2017). Integrated Data Sharing in the Context of Contemporary HCSC Networks

2) *Proliferation of Digital Health Information Across Multiple Providers*

With the digitization of healthcare, there is such an explosion in data sharing between consumers and multiple healthcare facilities. Figure 2 shows that a single patient, for instance, Seth, a student-athlete, will interact with many healthcare providers and organizations, all of which create, process, and disseminate vital health information. This is a complex model of modern healthcare delivery, with clinics, emergency departments, athletic facilities, and urgent care centers all essential parts of the system focused on maintaining patients' health (Dimitrov, 2016). The Nevada Spine Clinic, Rush University ER, DU. The Athletic Department and Las Vegas Quick Care are separate entities in Seth's healthcare network, each with relevant information about Seth.


Las Vegas Ortho Clinic
Sample Data Exchange Between the Patient and Organizations
Rush University ER
Nevada Spine Clinic 7140 Smoke Ranch Rd ...
Rush University Medical Group ...
QuickCare
DU Athletic Department
Seth is a student athlete
Las Vegas Quick Care

a) *Figure 2. An Example of Data Exchange between a Patient, His School, and Health Providers*

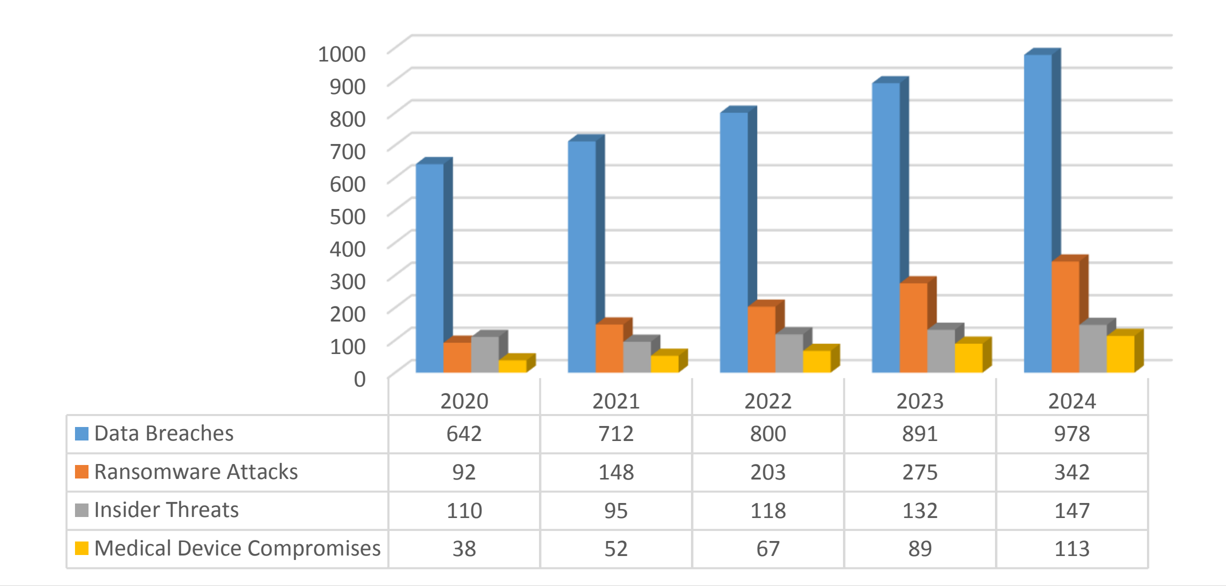
Mobile digital health data, among many suppliers, has its benefits and drawbacks. On the one hand, it can provide a more fabulous look at a particular patient's health condition, contributing to understanding when developing an individual approach and planning. In their study, Kotz et al. (2016) indicate that this integration can ensure that all healthcare consumers have the most up-to-date and relevant information to improve consumer outcomes. On the other hand, let me also note that the original interconnectedness of data exchange points is a vulnerability, as every connection point can be exploited. In this sense, the idea of interconnectedness, which marketers believe, is dangerous for IT systems.

Another layer of complexity arising from data flows is that different healthcare companies have adopted different levels of cybersecurity. Small clinics like Nevada Spine Clinic may not be able to implement robust cybersecurity systems compared to large organizations like Rush University Medical Center, as observed by Williams and Woodward (2015). Due to this mismatch of security capabilities, the broader healthcare data ecosystem has vulnerabilities, meaning that data that requires high-security access or is prone to security threats may be exposed.

Maintaining a uniform set of data protection standards is even more challenging because diverse organizations provide patient care. Emergencies focus on urgent care, and what is essential for an athletic department could be preventing sport-related injuries or an athlete's performance. Both perspectives could be balanced and ensured that all those involved strictly adhere to data security protocols throughout the healthcare network, maintaining the integrity and security of patient information (Martin et al., 2017).

3) *Vulnerabilities in Multi-Institutional Data Sharing Practices*

The progression of Seth's interactions with his athletic department and various medical facilities revealed highly susceptible multi-institutional data-sharing networks, which are depicted. These vulnerabilities result from various security measures, protocols, and systems that various organizations employ, leading to latent weak areas that malicious players may exploit. As Kruse et al. (2017) highlighted, the variability in IT systems and security management in different healthcare organizations amplifies the probability of incidents such as data breaches and unauthorized access to patients' information.



	2020	2021	2022	2023	2024
🟦 Data Breaches	642	712	800	891	978
🟧 Ransomware Attacks	92	148	203	275	342
⬜ Insider Threats	110	95	118	132	147
🟨 Medical Device Compromises	38	52	67	89	113

a) *Figure 3: Cybersecurity Incidents in Healthcare Organizations (2020-2024)*

Data Source: Using information from KPMG (2015), IBM Data Breach Calculator (n.d.), and Health IT (n.d.)

The rise of new threats in healthcare organizations over the last five years demonstrates the new challenges that interrelated healthcare systems face. The spectrum of data obtained from publications of KPMG (2015), IBM Data Breach Calculator (n.d.), and Health IT (n.d.) depict a worrying tendency. Thirty-eight medical devices were hacked, ten insider threats, 92 ransomware attacks, and 642 reported data breaches in 2020. These figures had sharply increased to 978 data breaches, 342 ransomware assaults, 147 insider threats, and 113 compromised medical devices by 2024. This sharp rise in sophistication and frequency of cyberattacks against healthcare organizations has been highlighted.

Healthcare providers' differing degrees of cybersecurity maturity are the main obstacles to protecting multi-institutional data sharing. Smaller clinics or sports departments might not have the resources or knowledge to implement as strong cybersecurity safeguards as larger academic medical centers like Rush University Medical Group. This discrepancy generates vulnerabilities that can be used to access the more extensive patient data network. Bell and Ebert (2015) have pointed out that hackers frequently target the weakest link in the healthcare data ecosystem, gaining access to more secure networks through hacked systems at smaller firms.

The intricate rules and agreements governing data exchange amongst several organizations add to the complexity of the security environment. Every step at which Seth's care providers exchange data with one another poses a risk that needs to be addressed appropriately. To safeguard these inter-organizational data transfers, burns et al. (2016) stress the significance of standardized data-sharing protocols and robust encryption techniques. Still, there is great difficulty in putting uniform security measures in place across various organizations with various IT infrastructures and operational priorities. The dramatic increase in ransomware attacks from 92 in 2020 to 342 in 2024 highlights the increasing risk to the availability and integrity of data in interconnected healthcare systems.

Furthermore, the fluidity of healthcare delivery—particularly in emergency scenarios or for athletes needing rapid attention—may encourage ad hoc data-sharing techniques that circumvent accepted security guidelines. Healthcare professionals may unintentionally expose patient information to dangers by cutting corners on data security procedures due to the demand to deliver care quickly. According to Shenoy and Appel (2017), one of the most critical issues facing healthcare cybersecurity is striking a balance between the necessity of quick information access in emergencies and strict data protection regulations. The rise in insider threats from 110 in 2020 to 147 in 2024 indicates that these demands, along with the possibility of malicious or human error, continue to be significant concerns to the security of patient data in multi-institutional settings.

4) *Potential Impact of Data Breaches on Patient Care Continuity*

The interconnectedness of healthcare data interchange, as described in Seth's story, highlights the need for data to be available and accurate to ensure continuity of care across different providers. The matters outlined in this context imply that several vital pieces of medical information that relate to Seth and the kind of treatment that he would be given might not only be disrupted but also significantly compromised if any of the organizations that he deals with were to fall victim of a data breach or cyber-attack. Martin et al. (2017) argue that one of the main challenges that put modern healthcare systems at risk is the possible disruption of patient care produced by cyberattacks.

The first data breach risk entails disclosing sensitive patient information, such as medical history and a treatment plan, and even identifying such a patient. However, this has implications that extend far beyond the matter of privacy. Patient records are vulnerable to cyber-attacks that could lead to clinical errors in diagnosis, treatment prescriptions, wrong care approaches, or delayed treatment. For example, according to Williams and Woodward (2015), the DU. The Athletic Department's decision-making process regarding Seth's participation in athletic activities could be severely affected if the data from his orthopedic evaluations at the Las Vegas Ortho Clinic were altered or rendered inaccessible. This, in turn, could endanger his health.

Because of how interconnected healthcare professionals are in managing a patient's health, a security compromise in one area might affect every step of the patient's treatment. There may be grave repercussions if the systems used at Rush University ER were to be hacked, especially when they could not find information relating to Seth's allergies or his medical history. Maintaining patient information consistency and access in all settings becomes critical, as Kotz et al. (2016) noted that an accurate and rapid exchange of information is essential to the emergency area.

Every facet of healthcare provision, from the management to services provision, poses a risk of data break, which may disrupt service delivery. Terrorists and hackers may threaten a client's financial position, delay getting treatment authorization, or even cancel appointments through cyber-attacks on charges, insurance data, and appointments. As Kruse et al. (2017) mentioned, due to our poor communication environment between healthcare and sports, Seth's rehabilitation and his performance on the sports field could be at risk if communication is disrupted. This may imply that he was unable to attend follow-up appointments or has not been receiving the therapies he requires.

5) Strategies for Enhancing Security in Interconnected Healthcare Systems

Consequently, there is a need to enhance security within health-affiliated networks such as Seth's network to counter the risks involved, hence the need for an over-arching quest to increase security. This strategy must balance one need to provide continuous data transmission with another need to protect patients' data to ensure that the quality and effectiveness of the treatment delivery is not compromised. The US Food and Drug Administration (2016) stated that there is a need for healthcare information technology cooperation between healthcare providers, technology vendors, and the authorities in formulating a solid healthcare system.

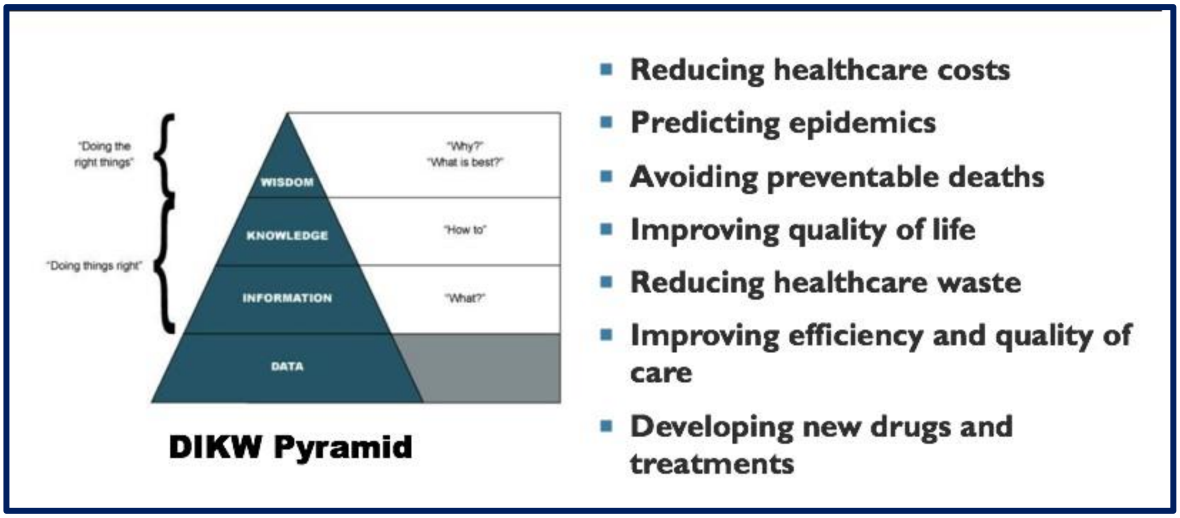
A primary tactic is the coordinated implementation of security measures and data exchange policies across all organizations involved in patient treatment. This includes establishing foundational security standards for participants in exchanging health information and ensuring all players, big and small – from large teaching hospitals to minor clinics, athletic departments, and guarantees – adhere to those standards. According to Burns et al. (2016), introducing a single system for risk evaluation and control of the healthcare system can help minimize potential danger points throughout the network and, in one way or another, reduce the opportunities for hackers to find 'loopholes.'

The use of complex encryption and authentication technologies has hence become necessary in enhancing the security of complex interlinked healthcare systems. Ensuring end-to-end encryption, including all the data exchanged between different healthcare providers, guarantees the confidentiality of such information, even if intercepted. Furthermore, two-factor authentication and segregation of duties significantly can reduce the chances of unauthorized access to the patient's information, even if a breach occurs at any of the affiliated businesses (Shenoy & Appel, 2017).

Real-time threat detection and constant monitoring abilities are crucial to maintaining the safety of interconnected healthcare systems. Experts at healthcare firms can use artificial intelligence and machine-learning models to detect real-time security events across their systems and infrastructures. Such a cybersecurity policymaking approach helps decrease the possible negative influence on patient care and data integrity by responding promptly to new threats. Moreover, participants also stated that simple security inspections or activities like penetration testing and security audits will aid in spotting and preventing these risks before being exploited by parties with ill intentions (Kotz et al., 2016). Maximizing Use of Data, Information, Knowledge, and Wisdom in the Healthcare Sector

6) *The DIKW Pyramid: A Framework for Healthcare Decision-Making*

In healthcare settings, the DIKW Pyramid is a helpful frame for understanding how the raw data could be transformed into actionable wisdom. Data—facts and numbers collected from many different locations across the healthcare continuum—are accumulated at the base of the pyramid. Only when data is put into context is it transformed into information. As one moves up the pyramid, it is converted to knowledge and then to wisdom that informs policy and direction in the health sector (Coulter et al., 2013). When it comes to cybersecurity, the timely interpretation of security-related data that could potentially make the difference between stopping a cyber-attack and becoming its next victim is where this move from data to wisdom is paramount.


"Doing the right things"
"Doing things right"
WISDOM
KNOWLEDGE
INFORMATION
DATA
"Why?" "What is best?"
"How to"
"What?"
DIKW Pyramid
Reducing healthcare costs
Predicting epidemics
Avoiding preventable deaths
Improving quality of life
Reducing healthcare waste
Improving efficiency and quality of care
Developing new drugs and treatments

a) *Figure 4. Data, Information, Knowledge, Wisdom Pyramid and How it Impacts Healthcare*

The DIKW Pyramid can be helpful in healthcare organizations and patient care. For instance, extracted data from medical devices and electronic health records can be preprocessed to make patient health patterns analytically useful. With professional experience, this data fosters knowledge used in therapy decisions. In conclusion, this knowledge shapes healthcare policy and guidelines, incorporating such information consistently and uniformly across cultures over time (Dimitrov, 2016). The DIKW framework is vital to any healthcare company's cybersecurity efforts. It helps healthcare companies analyze the threat landscape and adopt risk mitigation measures beyond collecting security log data.

7) *Transforming Healthcare Data into Actionable Intelligence*

Connecting real-time healthcare data with knowledge is vital for improving the quality of patient care, optimizing organizational workflows, and enhancing security. This transition commences with accumulating enormous data from several sources, such as electronic health records, medical instruments, and administration systems. However, the real value is revealed when the data is analyzed and put into a usable format. For instance, the regularity of patients' records allows for identifying disease evolution or treatment efficiency, while access patterns providing information about system usage may inform of security vulnerabilities (Kotz et al., 2016).

The process of moving up the DIKW Pyramid provides healthcare organizations with the knowledge that can be used to optimally manage the patient's welfare, resources, and security. This knowledge is obtained from merging information, clinical skills, and industrial practices. For instance, comprehending ordinary assault patterns and vulnerabilities within healthcare organizations might assist in developing better cybersecurity strategies (Kruse et al., 2017). The highest motivation is knowledge and wisdom, understood as the ability to use information in decision-making, solving complex problems, and making wise decisions. In the case of healthcare cybersecurity, wisdom may be understood as the capability of using preventive measures that would predict potential risks in advance and prevent their occurrence.

Turning data into insight is cyclical and requires constant continuous learning to improve effectiveness. By incorporating these strategies, the DIKW Pyramid can be implemented entirely in healthcare companies if they invest in a superior analytics department, encourage the use of data to make decisions, and prioritize cybersecurity in the industry. This enables them to enhance the likelihood of offering customer-focused quality patient care while safeguarding the integrity and confidentiality of consumer's health details from advanced IT threats (Williams & Woodward, 2015).

8) Implementing DIKW Principles to Enhance Healthcare Cybersecurity

Applying the principles of the DIKW Pyramid methodology has relevance to healthcare organizations' cybersecurity and has the potential to enhance an organization's capacity for protecting patient data and critical systems. Careful and comprehensive security information must be collected to get a broad picture of the current events: system logs, traffic statistics, and user activity records. This raw data is used for all subsequent security investigations and interventions. This data becomes essential information as it is scrubbed and processed to identify patterns of regular system operation and the potential for compromised security (Martin et al., 2017). This strategy is especially poignant given the recent rise in healthcare-specific cyberattacks. As stated by the data obtained from the KPMG's report (2015), IBM Data Breach Calculator(n.d.) and Health IT (n.d.) proposed that data breaches, for instance, escalated from 642 in the year 2020 to 978 in the year 2024. In contrast, ransomware attacks rose steeply from 92 to 342 in 2024.

Table 1: *Healthcare Cybersecurity Incidents and Their Impact (2020-2024)*

Year	Data Breaches	Ransomware Attacks	Insider Threats	Medical Device Compromises	Estimated Financial Impact (Millions USD)
2020	642	92	110	38	1,200
2021	745	178	125	52	1,850
2022	836	245	139	79	2,400
2023	912	298	144	96	3,100
2024	978	342	147	113	3,750

Source: *Compiled from reports by KPMG (2015), IBM Data Breach Calculator (n.d.), and Health IT (n.d.)*

The healthcare business will face new challenges in protecting patient information and essential systems, as depicted by this table revealing the rising rate of cybersecurity threats from 2020 to 2024. The data can be used to create a graph showing the changes in different cybersecurity threats over the years and the increasing costs affecting healthcare organizations.

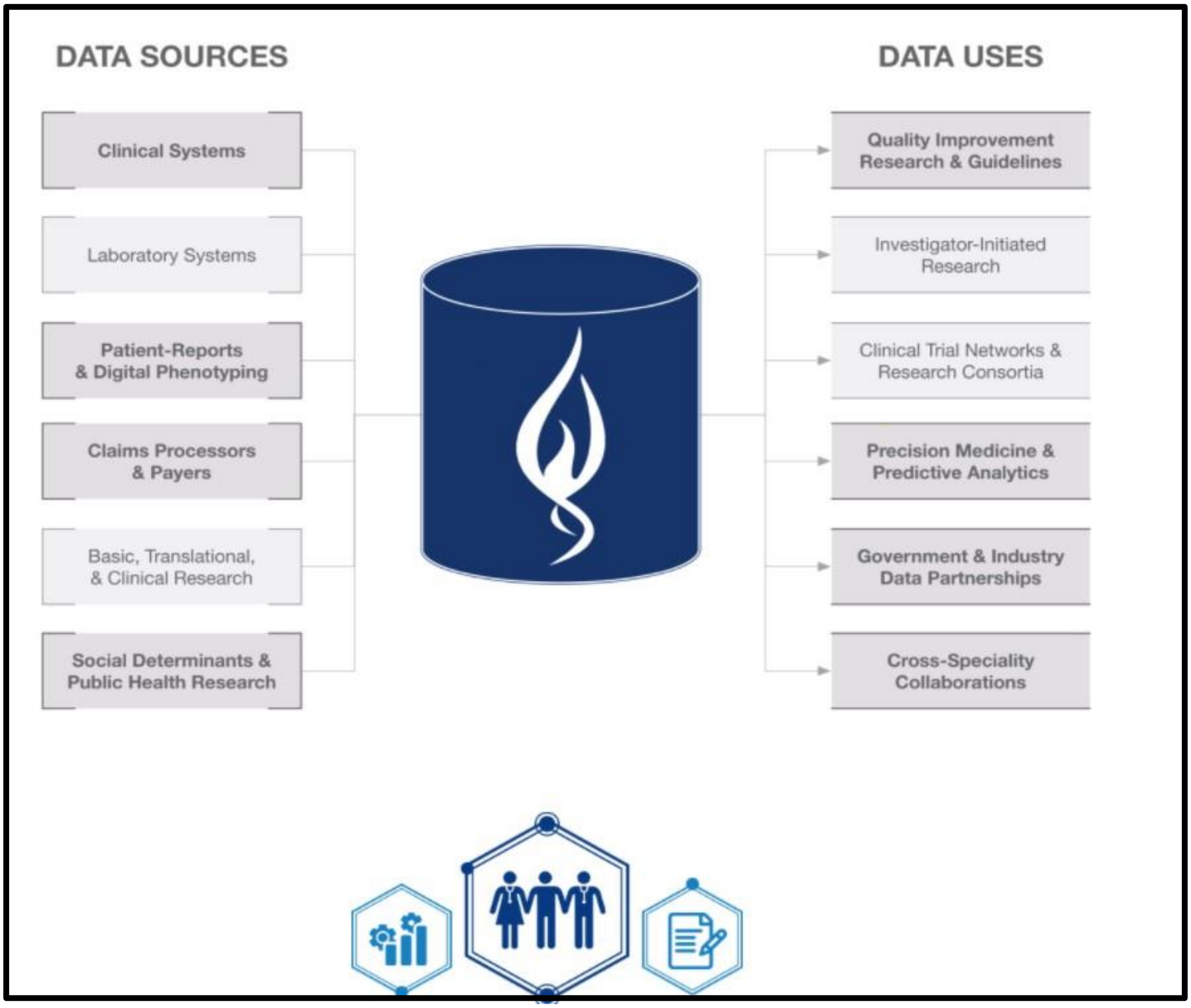
Security information transformed into knowledge and moving up the pyramid can be achieved by incorporating security data to understand cybersecurity threats, threat actors, and fields of specialization in healthcare firms better. This information makes it easier to note threats and deal with any incident. For example, enhanced intrusion identification and safety measures may help healthcare firms if their representatives know accepted cyber-attack practices (Burns et al., 2016). Regarding the cybersecurity resolve of the DIKW Pyramid, the degree of working wisdom is to look at security problems on the horizon and address them before they transform into threats. The rise in frequency of the threat enacted by insiders (from 110 in 2020 to 147 in 2024) and medical devices (from 38 in 2020 to 113 in 2024) is evidence of the importance of this knowledge.

The implementation of DIKW principles in healthcare cybersecurity requires a people-flow-technology approach. Modern Security Information and Event Management (SIEM) systems should be a priority for healthcare organizations. These systems should be able to instantly gather and analyze massive volumes of security data. Establishing reliable procedures for transforming security data into valuable insights is also essential. This entails conducting security assessments regularly, practicing threat modeling, and holding strategic planning meetings that use data-driven insights.

A healthcare provider should prioritize training its employees to be cybersecurity experts who can adequately understand, analyze, and respond to security intelligence (Shenoy & Appel, 2017). According to the data, the growing cost of cybersecurity incidents—a projected $1.2 billion in 2020 and $3.75 billion in 2024—highlights the critical need for this strategy. Healthcare companies must utilize the DIKW Pyramid to strengthen and fortify their cybersecurity measures to safeguard patient data and ensure this alarming growth underscores the continuity of healthcare services.

Leveraging Data Platforms for Healthcare Initiatives and Research

Medical data collection, analysis, and utilization have come a long way by introducing comprehensive data systems like Prometheus Research's RexRegistry into the healthcare system. As seen in Figure 5, these platforms function as consolidated databases that compile information from many sources. Among these are clinical and laboratory systems, patient-reported outcomes, claims processors, social determinants of health, basic and clinical research, and clinical and laboratory research. According to Dimitrov (2016), platforms like RexRegistry combine several data sources to generate a comprehensive dataset with multiple dimensions. This dataset has numerous potential uses in the healthcare industry. Researchers, policymakers, and healthcare professionals can better understand patient populations, treatment effectiveness, and public health trends by comprehensively integrating data.


DATA SOURCES
DATA USES
Clinical Systems
Laboratory Systems
Patient-Reports & Digital Phenotyping
Claims Processors & Payers
Basic, Translational, & Clinical Research
Social Determinants & Public Health Research
Quality Improvement Research & Guidelines
Investigator-Initiated Research
Clinical Trial Networks & Research Consortia
Precision Medicine & Predictive Analytics
Government & Industry Data Partnerships
Cross-Speciality Collaborations

a) *Figure 5: "RexRegistry" is a platform promoted by the business Prometheus Research. This platform provides its subscribers with high-quality data that can be utilized for various purposes, including study, activism, and teaching. Accessed at: https://www.prometheusresearch.com/*

These integrated data systems have way more uses than typical clinical research. The data used includes several diverse fields. These are investigator-initiated studies, precision medicine, community clinical trial groups, studies on quality and guidelines, and multidisciplinary collaborations. Thus, the opportunities for the widespread application of large interdisciplinary platforms, including comprehensive data platforms, are endless, emphasizing their immense potential to transform healthcare. Improved clinical methods may also benefit patient care, for example, if quality improvement research could employ real-world data (Kotz et al., 2016).

Using these platforms in the context of precision medicine and predictive analysis can revolutionize standard treatment practices by improving individual conformity in various aspects, such as medical record traits and tendencies.

One of the greatest strengths is the flexibility of such platforms as RexRegistry, which can facilitate inter-disciplinary collaboration and foster data-sharing between the government and the industry. These platforms enable the involvement of different specialists and enhance interdisciplinary approaches to healthcare research and innovation by using a common database and standard data analysis instruments. This erases silos between various approaches to medicine and scientific research institutions (Kruse et al., 2017).

This potential is indisputable on complex health issues requiring an understanding of several branches. Hypotheses assessed by analyzing different data sources will yield more improved, less exceptional results if the collection and analysis methods are unified. This enhances the generalizability of the findings in the various local and international studies.

Table 2: *Key Features and Applications of Comprehensive Healthcare Data Platforms*

Feature	Description	Primary Use Cases	Potential Benefits	Key Challenges
Data Integration	Aggregation of data from multiple sources	Research synthesis, Population health management	Holistic patient insights, Improved care coordination	Data standardization, Interoperability issues
Real-time Analytics	Continuous analysis of incoming data	Clinical decision support, Epidemic surveillance	Rapid response to health trends, Proactive care interventions	Data volume management, Algorithmic bias
Cross-specialty Access	Shared data access across medical specialties	Collaborative research, Multidisciplinary care approaches	Comprehensive treatment strategies, Innovation in care delivery	Data governance, Access control
Predictive Modeling	Use of historical data to forecast health outcomes	Risk stratification, Personalized medicine	Early intervention strategies, Optimized resource allocation	Model accuracy, Ethical implications
Patient-reported Outcomes	Integration of patient-supplied health data	Patient engagement, Symptom tracking	Patient-centered care, Improved treatment adherence	Data reliability, Patient Education
Regulatory Compliance Tools	Features ensuring adherence to healthcare regulations	HIPAA compliance, Ethical research practices	Protected patient privacy, Legal risk mitigation	Evolving regulations, international data sharing
Data Visualization	Tools for graphical representation of complex datasets	Trend analysis, Stakeholder communication	Intuitive data interpretation, Effective reporting	Information overload, Misinterpretation risks
Machine Learning Integration	AI-driven data analysis capabilities	Pattern recognition, Automated diagnostics	Enhanced diagnostic accuracy and efficiency in data processing	Algorithm transparency, Integration with clinical workflows

Source: *Compiled based on features commonly found in healthcare data platforms like RexRegistry and industry standards.*

Nevertheless, concerns about data security and privacy, as well as the ethical utilization of patient data, arise regarding the application of extensive data platforms. Security procedures are needed to protect the patients' information because these centralized platforms collect private health information from various sources and attract hackers' attention (Williams & Woodward, 2015). Moreover, patient identification and data security must be addressed to avoid violating patients' rights and confidentiality. Legal requirements such as HIPAA should always be followed when using patients' data for research and commercial purposes. The many benefits of using these outlets offer a pivotal strength to data consumption in the fast-evolving healthcare environment. However, moderating the risks that come with it while observing patient rights and data security remains paramount.

CHALLENGES & STRATEGIES

C. 4.1 Challenges in Implementing Comprehensive Cybersecurity Measures in Healthcare

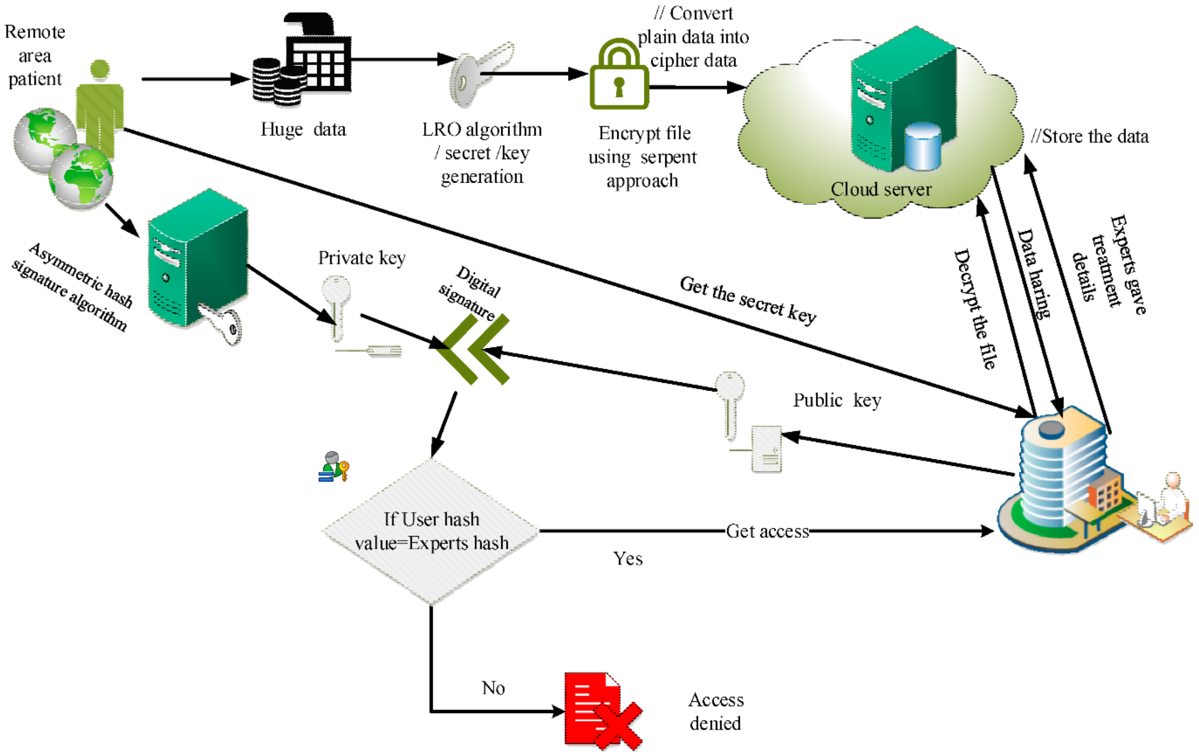
Due to the critical role of healthcare products and services, rigorous legal requirements, and the complexity of the field, it is challenging to incorporate robust cybersecurity measures into healthcare organizations. They are maintaining what one can call the 'security balance,' which is the other challenge in ensuring that efficient, secure, and accessible healthcare delivery is achieved. For effective and timely treatment, medical professionals require immediate data access from patient records that, many times, potentially conflicts with security standards. Accompanying the general tension between making data available and protecting them from unauthorized access, there is even increased tension where, for instance, any delay in information access can cost human lives, which brings to light discussion from Kotz et al. (2016). In addition, the high degree of diversification of the IT equipment used at healthcare facilities makes protecting all utilized devices and systems challenging. These devices include legacy, first-generation IoMT, and advanced, new-generation IoMT devices.

The healthcare industry's scarcity of qualified cybersecurity professionals is another major obstacle. Competition from other sectors and limited funds make it difficult for healthcare businesses to recruit and retain experienced cybersecurity personnel (Landi, 2015). Due to a lack of trained personnel, numerous healthcare facilities are susceptible to complex cyberattacks. Additionally, while healthcare data protection regulations are essential, they might sometimes slow the implementation of new security measures. Implementing security measures may be hindered by the need to carefully evaluate and comply with rules like HIPAA in the US. The coordination of actions across many jurisdictions and healthcare systems is further complicated by the worldwide character of cyber threats (Shenoy & Appel, 2017).

In healthcare cybersecurity, the human element is still a central weak spot. Because their primary attention is on the patients, healthcare workers might not always put cybersecurity first. Although it is crucial, it can be challenging to effectively execute training programs that increase awareness and enhance cybersecurity hygiene among healthcare personnel in extensive and diverse companies. The COVID-19 pandemic and other recent events have hastened the shift toward remote work and telemedicine, increasing the attack surface for healthcare institutions. Additional complexity to healthcare cybersecurity initiatives is the need to secure remote access points and guarantee the privacy of telehealth consultations (Hackett, 2020). To build a resilient defense against developing cyber threats in the healthcare sector, addressing these complex issues through a multi-pronged strategy that includes technological solutions, staff training, policy implementation, and industry-wide collaboration is necessary.

4.2 Strategies for Enhancing Healthcare IT Cybersecurity

1 **Implementing Multi-layered Security Measures:** A robust cybersecurity plan for hospital IT systems must integrate many layers of protection, as depicted in Figure 6. This method initiates safeguarding remote patient data via encryption and secure transmission mechanisms. The model explores how patient data is encrypted before storing it in the cloud servers using methods such as LRO and the Serpent method. Also, the efforts to add asymmetric hash signature techniques in authentication increase safety. This multiple-layered approach helps to protect against as many possible intrusions as possible. It ensures that even if one layer is penetrated, other layers will continue to protect the system from hackers or data leakage (Kotz et al., 2016).


Remote area patient
Huge data
LRO algorithm / secret /key generation
// Convert plain data into cipher data
Encrypt file using serpent approach
Cloud server
//Store the data
Experts gave treatment details
Data haring
Decrypt the file
Get the secret key
Asymmetric hash signature algorithm
Private key
Digital signature
Public key
If User hash value=Experts hash
Get access
Yes
No
Access denied

a) Figure 6. Model of security system in innovative hospital management

2 **Utilizing Advanced Encryption and Access Control:** As illustrated in Figure 6, protecting private health information requires much reliance on encryption. The model demonstrates how public and private critical systems can control access and safely transfer information. Healthcare organizations should adopt effective channel and database encryption to ensure that, if data is intercepted, it remains meaningless to illicit individuals. Expert hash value verification, illustrated in the figure, is one of the measures that ensure only the permitted individuals affect privileged data. This strategy corresponds to guidelines for protecting the ePHI according to the recommendations of the US Department of Health and Human Services (2016).

3 **Adopting Cloud-based Security Solutions:** The intelligent hospital management strategy in Figure 6 employs cloud servers for data storage and processing. There are many advantages for healthcare organizations in using cloud-based security solutions, including the ability to scale up or down quickly and automatically and alert the organization to more complex threats. To ensure that cloud providers are HIPAA compliant, it is necessary to check that they agree with healthcare guidelines. Healthcare businesses must implement additional security measures, such as data encryption, before storing the data in the cloud and managing the keys, as shown in the model. This method allows healthcare practitioners to tap into the benefits of cloud computing, strictly controlling patients' essential data (Williams & Woodward, 2015).

4 **Implementing Robust Authentication Mechanisms:** The effect of better authentication on healthcare IT systems is illustrated in Figure 6. One of the phases in the model is the process of checking where user hash values match expert hash values before granting access. Healthcare companies should use multi-factor authentication, or MFA, for any user accessing sensitive systems or data. This might also consist of regular passwords, smart cards, biometrics, or token systems. Sound authentication practices help minimize illegitimate attempts when credentials

may be compromised. Furthermore, role-based access control enables access control that ensures that the users can only access the data needed for specific job roles (Kruse et al., 2017).

5 **Continuous Monitoring and Threat Detection:** One could explain that constant monitoring and threat identification should be elements of a good healthcare cybersecurity strategy, although they are not depicted in Figure 6. Healthcare organizations should incorporate modern SIEM systems into their networks to track user activity, system and network event logs, and real-time traffic. Some kind of security risk may be present if some activity signs are seen that are out of the ordinary, and this can be discovered using machine learning and AI. Addressing security threats before they occur allows for prompt responses to potential security threats, thus maintaining the delivery of essential healthcare services and reducing the consequences of breaches (Martin et al., 2017).

6 **Regular Security Assessments and Updates:** The security model portrayed in Figure 6, created by healthcare companies, must often undergo security assessments to ensure that every system is updated consistently. This includes activities such as the assessment of web application, network, and system vulnerability, which involve the following tasks: penetration testing, vulnerability scanning, and third-party security audits. The regular assessments help the system identify various potential weaknesses in the security architecture before nasty actors seize the opportunities. A robust security position also means that every system, including IoT and medical, must be updated with the latest security patch. Healthcare IT on the state of security threat must constantly evaluate and enhance to stay relevant (Burns et al., 2016).

II. 5. Conclusion and Recommendations

5.1 Conclusion

In conclusion, the healthcare industry is in a precarious position in the current period of technological advancement and rising cybersecurity threats. This exhaustive research sheds light on the complex and complex nature of the cybersecurity threats that healthcare businesses meet today. Threats are diverse; they are dynamic, for instance, never-a-day cyber node attacks and the increased application of linked medical devices. This is especially true today, given the rising cases of data theft, ransomware attacks, and the recent compromises of medical devices. Maintaining a proper fit between data availability and data security is a tricky knot that healthcare providers must solve while striving to implement big data and analytics to improve patient care. Although the DIKW Pyramid is a useful model that helps transform raw data into valuable knowledge, it also reveals how unsound data is at each level of its analysis. To maintain the stability and safety of patient care in the healthcare sector, the focus should be on constant and all-encompassing IT security protocols necessary in modern healthcare. This includes technology, human factors, and plans for the future.

5.2 Recommendations

To address the cybersecurity challenges in healthcare IT firms, they need to establish the Zero Trust Architecture. This strategy mandates that the principle 'never trust, always verify' be applied to all network end users through multi-factor authentication; essential systems should be segregated through micro-segmentation. The administrative controls must be checked and modified periodically to maintain the concept of least privilege.

Improving the security of medical devices is essential. Healthcare providers should perform the proper cybersecurity check on all linked devices, cooperate with manufacturers to provide adequate security updates, and limit these devices' access to the hospital network. A key element includes the continuous inventory of all contact points and the associated devices, particularly their security status and patch level.

Investing in building threat detection and response capacity and infrastructure is pertinent. This includes introducing Security information and event management powered by artificial intelligence that helps identify threats in real-time and establishing a security operation center that operates round the clock. Automated processes for responding to incidents should be developed to minimize the time required to address possible threats. Daily penetration testing and vulnerability assessments will help in avoiding such issues in the future.

Successful data governance is consequently essential: A comprehensive data governance approach is required. This plan should contain policies addressing data classification, usage, and access issues. Measures against data leaks can reduce unlawful data transfers, but ensuring encryption of all critical data, including stored and transmitted, can be necessary. Approving data access logs frequently and applying an anomaly detection system assists in identifying insider threats.

A strong defense entails creating a cybersecurity awareness culture. This encompasses insisting on firmwide compulsory, position-sensitive information security training for all personnel, engaging in occasional simulated phishing and security consciousness activities, and defining clear procedures for reporting security incidents. The principle of cybersecurity should make it a part of any healthcare process and management.

Another primary concern, for instance, concerns the enhancement of supply chain security. Healthcare companies must actively ensure and protect all third parties and partners they work with, set high-security requirements for all vendors, and periodically review the accessibility of the healthcare company's systems and data by third parties. This also involves building the capability of anticipatory supply chain risk management strategies to counter expected supply chain threats or vulnerabilities.

An effective incident reaction and recovery play a crucial role in ensuring resilience. This plan should cover all aspects, be run through and evaluated frequently, and contain safe off-site data backups and the testing of the restoration procedures. Appropriate procedures for informing the patient, the personnel, and other regulatory organizations should be set up in case of a breach since an increase in post-breach notifications and post-breach analysis improves the response mechanism.

Advanced technology can significantly enhance the level of protection. Three areas applicable to implementation in healthcare organizations are Blockchain for the secure exchange of Health Information, machine learning algorithms for predictive threats analysis, behavioral analysis for detection of abnormal activities, and quantum-resistant encryption for future security.

Therefore, the best approach to dealing with emerging dangers is to collaborate closely with allies in industry and the regulatory agencies. In the identified area of focus, healthcare providers should actively participate in threat intelligence sharing initiatives that are relevant to the healthcare sector, become involved in the development of future rounds of regulation, collaborate with academic institutions that have expertise in cutting-edge research, and share knowledge with other healthcare providers and cooperate with other healthcare organizations where such collaboration will be mutually beneficial.

Lastly, privacy-preserving technologies must be underlined as essential in the context of big data. The recommendations for improving healthcare's approaches to privacy include applying differential privacy to big data analytics, exploring homomorphic encryption for the secure computation of data, applying the privacy by design principle on all new IT solutions, and continuously conducting privacy impact assessments on all data-related projects. These extensive recommendations would enable healthcare companies to bolster their cybersecurity exceptionally, safeguard patient information and guarantee the sustainability of critical healthcare services in a more connected and digitalized world.

vices in a more connected and digitalized world.

Bibliographies

Abelson, R., & Goldstein, M. (2015). Anthem hacking points to security vulnerabilities in the healthcare industry. *New York Times*. http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html

Armstrong, S. (2018). Data deadlines loom large for the NHS. *BMJ*, p. *360*, k1215. https://doi.org/10.1136/BMJ.K1215

Arndt, R. Z. (2018). In healthcare, breach dangers come from inside the house. *Modern Healthcare*. http://www.modernhealthcare.com/article/20180410/NEWS/180419999

Bell, G., & Ebert, M. (2015). *Health Care and Cyber Security*. https://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf

Berlinger, J. (2016). Justice Department files record $900 million healthcare fraud case. *CNN*. http://edition.cnn.com/2016/06/23/health/health-care-fraud-takedown/index.html

Burns, A. J., Johnson, M. E., & Honeyman, P. (2016). A brief chronology of medical device security. *Communications of the ACM*, *59*(10), 66–72. https://doi.org/10.1145/2890488

Conn, J. (2016). Data breach affects 12,000 patients in New Mexico substance-abuse program. *Modern Healthcare*. http://www.modernhealthcare.com/article/20160523/NEWS/160529984

Coulter, A., Roberts, S., & Dixon, A. (2013). *Delivering Better Services for People with Long-Term Conditions Building the House of Care*. https://www.kingsfund.org.uk/sites/default/files/field/field_publication_file/delivering-better-services-for-people-with-long-term-conditions.pdf

Cybersecurity in healthcare threats and impact. (n.d.). GE Healthcare. https://www.gehealthcare.com/infographics/infographic-cybersecurity-in-healthcare---threats-and-impact

Deane-McKenna, C. (2017). NHS ransomware cyber-attack was preventable. *The Conversation*. http://theconversation.com/nhs-ransomware-cyber-attack-was-preventable-77674

Dimitrov, D. V. (2016). Medical internet of things and big data in healthcare. *Healthcare Informatics Research*, *22*(3), 156-163. https://doi.org/10.4258/hir.2016.22.3.156

Dobrin, B. (2019). 31 Must know cybersecurity statistics. Phoenix Nap. https://phoenixnap.com/blog/healthcare-cybersecurity-statistics

Evenstad, L. (2016). NHS trust recovers after cyber-attack. *Computer Weekly*. http://www.computerweekly.com/news/450402278/NHS-trust-recovers-after-cyber-attack

Fraud watch. (n.d.). COVID-19 has long-term effects on cybersecurity. https://fraudwatchinternational.com/active-scams/covid-19-has-long-term-effects-on-cyber-security/

Hackett, M. (2020). Cybersecurity attacks have increased during the COVID-19 crisis: Hackers use provider distraction to breach health systems. *Healthcare Finance*. https://www.healthcarefinancenews.com/news/number-cybersecurity-attacks-increase-during-covid-19-crisis

Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., Fu, K., Kohno, T., & Maisel, W. H. (2008). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *2008 IEEE Symposium on Security and Privacy* (pp. 129-142). IEEE. https://doi.org/10.1109/SP.2008.31

Health Care Industry Cybersecurity Task Force. (2017). *Report on Improving Cybersecurity in the Health Care Industry*. https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

Health IT (n.d.). Laws, Regulation and Policy. https://www.healthit.gov/topic/laws-regulation-and-policy

Health IT (n.d.). Privacy, Security and HIPAA. https://www.healthit.gov/topic/privacy-security-and-hipaa

Healthcare cybersecurity. (n.d.). Fortinet. https://www.fortinet.com/solutions/industries/healthcare.html?utm_source=blog&utm_campaign=2018-q2-healthcare-page

HHS. (2016). *Ransomware and HIPAA*. https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

IBM Data Breach Calculator. (n.d.). https://databreachcalculator.mybluemix.net/

Kam, R. (2015). The human risk factor of a healthcare data breach – Community Blog. *IT Exchange*. https://searchhealthit.techtarget.com/healthitexchange/CommunityBlog/the-human-risk-factor-of-a-healthcare-data-breach/

Kangas, E. (2017). Why Are Hackers Targeting Your Medical Records? https://luxsci.com/blog/hackers-targeting-medical-records.html

Kloof, D. C. (2015). Cybersecurity for connected diabetes devices. *Journal of Diabetes Science and Technology*, *9*(5), 1143-1147. https://doi.org/10.1177/1932296815583334

Kotz, D., Gunter, C. A., Kumar, S., & Weiner, J. P. (2016). Privacy and security in mobile health: a research agenda. *Computer*, *49*(6), 22-30. https://doi.org/10.1109/MC.2016.185

KPMG. (2015). *Health Care and Cyber Security: Increasing Threats Require Increased Capabilities*.

Kruse, C. S., Frederick, B., Jacobson, T., & Monti cone, D. K. (2017). Cybersecurity in healthcare: a systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10. https://doi.org/10.3233/THC-161263

Kumari, A., Tanwar, S., Tyagi, S., & Kumar, N. (2019). Verification and validation techniques for streaming big data analytics on the Internet of Things environment. *IET Networks*, *8*(3), 155–163. https://doi.org/10.1049/iet-net.2018.5187

Landi, H. (2015). The healthcare industry faces a shortage of experienced cybersecurity experts. https://www.healthcare-informatics.com/news-item/healthcare-industry-faces-shortage-experienced-cybersecurity-experts

Leffel, C. (2017). Healthcare Cybersecurity: 10 Tips for Keeping Private Health Data Secure. HIT Consultant. https://hitconsultant.net/2017/07/25/tips-private-health-data-secure/#.Xo-EstOpGCU

Levin, D. Z., & Christmann, P. (2006). Institutionalism, Learning, and Patterns of Decoupling: The Case of Total Quality Management.

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *BMJ*, p. *358*, j3179. https://doi.org/10.1136/BMJ.J3179

Munro, D. (2014). Cyber-attack nets 4.5 million records from large hospital systems. *Forbes*. http://www.forbes.com/sites/danmunro/2014/08/18/cyber-attack-nets-4-5-million-records-from-large-hospital-system/#6740d5cd18bc

Murray, K. (2019). Why healthcare organizations are easy targets for cybercrime. Webroot. https://www.webroot.com/blog/2019/10/24/why-healthcare-organizations-are-easy-targets-for-cybercrime/

National Audit Office. (2017). *Investigation: WannaCry Cyber Attack and the NHS*. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS-Summary.pdf

Newman, L. H. (2017). Medical Devices Are the Next Security Nightmare. *Wired*. https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

Orcutt, M. (2014). 2015 could be the year of the hospital hack. *MIT Technology Review*. https://www.technologyreview.com/s/533631/2015-could-be-the-year-of-the-hospital-hack/

Parmar, A. (2012). Hackers show off vulnerabilities in wireless insulin pumps. *Med City News*. https://medcitynews.com/2012/03/hacker-shows-off-vulnerabilities-of-wireless-insulin-pumps/

Pycroft, L., Boccard, S. G., Owen, S. L. F., Stein, J. F., Fitzgerald, J. J., Green, A. L., & Aziz, T. Z. (2016). Brain jacking: Implant security issues in invasive neuromodulation. *World Neurosurgery*, pp. *92*, 454–462. https://doi.org/10.1016/j.wneu.2016.05.010

Ross, R. S., Feldman, L., & Witte, G. A. (2016). Rethinking Security Through Systems Security Engineering. *ITL Bulletin – December 2016*. https://www.nist.gov/publications/rethinking-security-through-systems-security-engineering

Scott, M., & Wingfield, N. (2017). The hacking attack has security experts scrambling to contain the fallout. *New York Times*. https://www.nytimes.com/2017/05/13/world/asia/cyberattacks-online-security-.html

Sengupta, K. (2017). Isis-linked hackers attack NHS websites to show gruesome Syrian civil war images. *The Independent*. http://www.independent.co.uk/news/uk/crime/isis-islamist-hackers-nhs-websites-cyber-attack-syrian-civil-war-images-islamic-state-a7567236.html

Shenoy, A., & Appel, J. M. (2017). Safeguarding confidentiality in electronic health records. *Cambridge Quarterly of Healthcare Ethics*, *26*(2), 337-341. https://doi.org/10.1017/S0963180116000931

Sienko, C. (n.d.). The Breach of Anthem Health. Infosec Resources. https://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-attack-statistics-and-case-studies/case-study-health-insurer-anthem/#gref

Sobers, R. (2020). Data Security: 107 Must-Know Data Breach Statistics for 2020. Varonis. https://www.varonis.com/blog/data-breach-statistics/

Storm, D. (2015). MEDJACK: Hacker's hijack medical devices to create backdoors in hospital networks. *Computerworld*, p. 8. https://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html

Suleyman, A. (2017). NHS cyber-attack: Why stolen medical information is much more valuable than financial data. *The Independent*. http://www.independent.co.uk/life-style/gadgets-and-tech/news/nhs-cyber-attack-medical-data-records-stolen-why-so-valuable-to-sell-financial-a7733171.html

Takahashi, D. (2011). Excuse me while I turn off your insulin pump. *VentureBeat*. https://venturebeat.com/2011/08/04/excuse-me-while-i-turn-off-your-insulin-pump/

The impact of technology in healthcare. (n.d.). AIMS Education. https://www.aimseducation.edu/blog/the-impact-of-technology-on-healthcare/

Trend Micro. (2018). Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101

US Department of Health and Human Services. (1996). Your Rights Under HIPAA. https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html

US Department of Justice. (2016). Three Individuals Charged in $1 Billion Medicare Fraud and Money Laundering Scheme. https://www.justice.gov/opa/pr/three-individuals-charged-1-billion-medicare-fraud-and-money-laundering-scheme

US Food and Drug Administration. (2014). *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff*. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf

US Food and Drug Administration. (2016). *Postmarked Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff Additional Copies*. https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf

Vasa, L. (2016). Hospitals are vulnerable to cyber-attacks on just about everything. *Naked Security*. https://nakedsecurity.sophos.com/2016/02/26/hospitals-vulnerable-to-cyber-attacks-on-just-about-everything/

Walker, T. (2017). Interoperability is a must for hospitals, but it comes with risks. *Managed Healthcare Executive*. http://managedhealthcareexecutive.modernmedicine.com/managed-healthcare-executive/news/interoperability-must-hospitals-it-comes-risks

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices (Auckland, NZ)*, pp. *8*, 305–316. https://doi.org/10.2147/MDER.S50048