AMERICAN JOURNAL OF INNOVATION IN SCIENCE AND ENGINEERING (AJISE)

ISSN: 2158-7205 (ONLINE)

VOLUME 3 ISSUE 3 (2024)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Innovation in Science and Engineering (AJISE)

Volume 3 Issue 3, Year 2024
ISSN: 2158-7205 (Online)
DOI: https://doi.org/10.54536/ajise.v3i3.3576
https://journals.e-palli.com/home/index.php/ajise

The Growing Cybersecurity Crisis in Healthcare: A Call to Action

Muritala Kolade Yusuf[1*], Ayuba Job Danladi[1], Emmanuel Song Shombot[2], Gilles Dusserre[2], Victoria Abeyi Odey[1], Nasir Baba-Ahmed[1], Robert Bestak[3], Mohammed Isa Lawan[1]

Article Information

Received: August 25, 2024
Accepted: October 01, 2024
Published: October 31, 2024

Keywords

Cyber-Attack, Cybersecurity, Data Encryption, Protected Health Information (PHI)

ABSTRACT

Electronic healthcare technology is pervasive throughout the globe, and it affords vast opportunities to enhance clinical outcomes, as well as for the transformation of models of care. Concerns are, however, growing, related to healthcare data and device security. Increased connectivity to legacy computer networks brought cybersecurity vulnerabilities for medical devices. Healthcare represents an attractive target for cybercrime because healthcare data is precious. This sector in present times is full of unique cybersecurity challenges, especially for susceptible kinds of patient information at stake. Second, many legacy systems will be prevalent—not adding more to that—with the changing face of cyber threats. Cybersecurity breaches have comprised stealing health information and focused ransomware attacks on hospitals; this could mean as vivid an attack as on implanted medical devices. This only points to the fact that ransomware attacks and other kinds of cyber-attacks against hospitals and other medical facilities are gaining ground; there is every reason to get alarmed and put in place stricter cybersecurity measures. An excellent healthcare cybersecurity strategy, therefore, has to consider access control, intrusion detection systems, encryption techniques, and periodic security testing. Data breaches and cyber-attacks are forcing any healthcare provider to invest in new state-of-the-art technologies related to keeping pace with trends regarding cybersecurity. The dangers that can be caused by cyber-attack include a considerable diminution in patient trust, potential health system collapse, human life threats, etc. On the whole, cybersecurity is strenuously linked with the question of patient safety.

INTRODUCTION

Through the integration of digital technology, the healthcare sector is fast evolving, improving efficiency and providing better patient care through streamlined operations (Senbekov *et al.*, 2020). Nowadays, cybersecurity is extremely important to medical institutions because data theft, data breaches, and ransomware attacks can affect a variety of sectors, including health departments, care providers, diagnostic services, research institutions, and primary healthcare practices (Mahmoud & Al-Najjar, 2024). Cybersecurity is a major concern for the healthcare industry as cyber-attacks targeting the healthcare industry have been increasing at an alarming rate around the world (Al-Qarni, 2023; Tin *et al.*, 2023). The healthcare sector throughout the world now prioritizes protecting patients' sensitive information, securing network infrastructure, and fighting against cyber-attacks (Bhosale *et al.*, 2021). The healthcare sector is a popular target for cyber-attackers due to the large amount of personal and health data it holds. A complex network of vulnerabilities that attackers can take advantage of is created by Electronic Health Records (EHRs), medical equipment, telemedicine channels, and associated networks (Yeng *et al.*, 2023; Haleem *et al.*, 2021). The threats that healthcare providers encounter daily include hacking, ransomware attacks, data breaches, and phishing attacks (Ahmed *et al.*, 2020). Our goal is to assess past and existing cyber-attacks targeted primarily on the health sector, to unravel the impact it has and continues to have on the health sector. The gap in this research area has over time, been given limited attention, and this continues to pose a huge threat to sensitive healthcare data, especially high-profile individuals that are often targeted for political reasons. Such gap needs to be filled to mitigate these attacks. Cyber-attacks in the healthcare industry have significant consequences, including operations disruption, patient care compromise, financial losses, damage to reputation, and endangering lives (Meisner, 2018). To protect healthcare institutions assets and minimize risks, healthcare companies are investing more in cybersecurity measures (Argaw *et al.*, 2020). Strong cybersecurity measures-such as access controls, encryption protocols, cybersecurity frameworks, cybersecurity training for the employees and regular security assessments-as well as compliance with regulations like the European GDPR (General Data Protection Regulation) and the US Health Insurance Portability and Accountability Act (HIPAA), are essential for ensuring the security and privacy of patients data (Mahmood *et al.*, 2019; Syafrizal *et al.*, 2022), however, the trends in these attacks tends to be on the rise, especially with rapid advancement in technologies. Our research seeks to explore sustainable cybersecurity measures that can be implemented in healthcare sectors, mitigation and to a greater extent eliminate such attacks. To establish a basis for our research, two research questions were defined to serve as a measuring scale for the outcome of our work.

RQ1: What types of cyber-attacks are targeted towards health sectors?

[1] IMT Mines Ales, France
[2] Laboratory for the Sciences of Risks, IMT Mines Ales, Ales, France
[3] Czech Technical University in Prague, Czech Republic
[*] Corresponding author's e-mail: yusufmur1113@gmail.com

RQ2: What is the trend of past and existing attack on the health sector?

This research is aimed at assess the types of cyber-attacks on healthcare institutions and their historical trend. This will guide an understanding of the urgent need to secure cyberspace data in the health sectors and lead to innovation of sustainable safeguarding measures for protecting healthcare information/data. We aim to achieve the following objectives

i. Collect data on incidents of cyber-attacks targeted on healthcare institutions

ii. Categorizing the various cyber-attack incidents and stating the types of attacks based on the attack vectors that cybercriminals use to attack the targeted entity

iii. To find trends among the cyber-attack occurrences that has impacted the healthcare industry

Definition of Terms

Cybersecurity

Healthcare cybersecurity is defined as the techniques and technologies used in defending organization networks, computer systems, databases, and health information systems against cyber-attacks, threats, unauthorized access, and damage (Kale *et al.*, 2022).

Cyber-Attack

A cyber-attack is an attack designed to steal, modify, or destroy all kinds of valuable data in computer information systems, infrastructures, networks, and personal computer devices. Without a doubt, no industry or sector is safe from cyber-attack, and the healthcare sector is no exception. It has remained under severe cyber-attack during the past few years. Most of the entities in the healthcare sector are not well prepared or fully equipped with resources to detect and prevent the possibility of cybersecurity incidents. Cybercriminals are taking advantage of the vulnerability in the healthcare sector to disrupt medical services and steal patients' Protected Health Information (PHI) (Swasey, 2020; Kale *et al.*, 2022).

Protected Health Information (PHI)

Protected Health Information (PHI) includes data identifying to a patient, such as name, birthdate, SSN, address, phone number, medical record, diagnostic test results, payment records, and photographs. This type of information shall not be disclosed or made known to unauthorized individuals (Moore & Frye, 2019).

LITERATURE REVIEW

To document past research on this topic, identified and reviewed the existing cyber-attack databases (shown in Table 1 below) by conducting a detailed web search for data within our defined criteria (see Table 2 and Table 3). The explored databases consisted of cyber-attack incidents that occurred on a global scale in various sectors such as Public Administration, Healthcare, Information, Education services, Manufacturing, Transportation, Finance and Insurance, Media, Professional/Scientific, etc. which we further streamlined to records containing only health sector attacks.

Table 1: Cyber-attack databases and their brief description

Database	Country covered	Brief description
University of Maryland CISSM cyber-attacks database.	Worldwide	This database is an all-inclusive source of information about incidences of cyber-attack occurrences. It spans through a broad range of occurrences of cyber-attacks in various industries: manufacturing, public administration, healthcare and social assistance, information, education services, finance and insurance, professional, scientific, and technical services. Some ways of categorizing the incidence of cyber-attacks are in terms of type of attack, the target industry or organization and the location, the motives of the attacker, the date the attack occurred etc. The database contains well-known cyber incidents of large-scale impact together with little-known cases that may give insight into new trends of emerging cyber threats.
U.S. Department of Health & Human Services - Office for Civil Rights.	United States	This database is a platform of tracking and reporting unsecured Protected Health Information (PHI) as mandated by the Health Insurance Portability and Accountability Act (HIPAA). The database includes breaches reported by healthcare providers, health plans, and healthcare clearinghouses and their business associates. The database includes such information as the name of the entity targeted, the type of breach, and the number of individuals whose information was affected etc.
European Repository of Cyber Incidents (EuRepoC).	Worldwide	This database serves as a valuable resource for all those who need cybersecurity, policy persons, and other stakeholders in support of their efforts for the protection of critical infrastructures, countering cyber risks, and enhancing cybersecurity resilience. This database keeps track of incidences of cyber-attacks from the year 2000 to date on educational institutions, media, scientific institutions, and other such entities. The repository harbors a broad range of cyber incidents, such as data theft hijacking involving misuse, ransomware, hijacking without misuse, etc.

Cyber Attacks in Times of Conflict compiled by CyberPeace Institute	Worldwide	This repository is a dedicated database for cyber-attack incidents within the context of political tensions, armed conflicts, or other forms of international disputes from January 2022 to December 2023. Dates of attacks, the country in which an attack occurred, sectors attacked, types of attacks, actors behind the attacks, impacts on the affected targeted entities, and people are some of the essential information pieces attached to each cyber-attack documented in the database.

MATERIALS AND METHODS

The first step of our method was to design a workflow for this work, by outlining each step, leading to achieving our aim. This workflow (Figure 1), provided a simplified guide for the fulfilling the objective in each section.

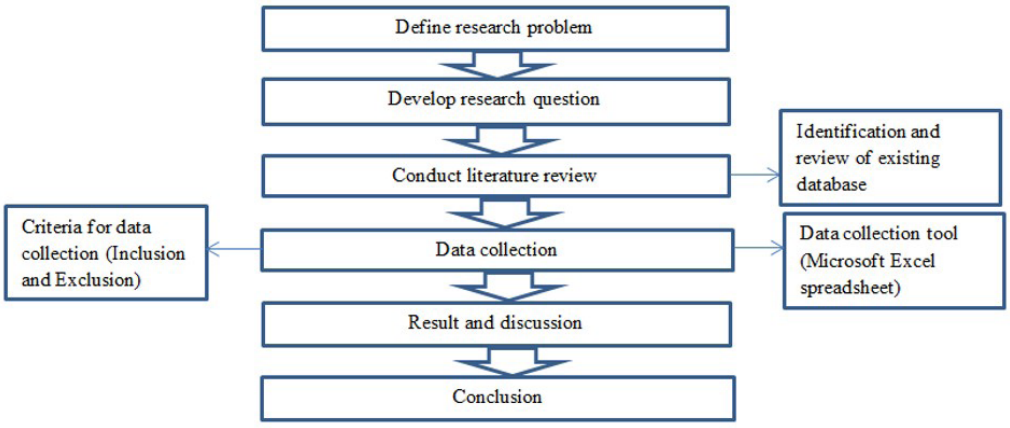

Figure 1: Research process flow chart

We proceeded to critically define the research problem and research questions. We then by identifying cyber-attack databases and other sources that contain cyber-attack incidents in the various sectors to access information by gathering the relevant data for our research subject. We relied on these databases and other sources on the fact that they contain genuine and verifiable information. During the data gathering, a search strategy including selection criteria to explore relevant studies was developed, as explained in Table 2 and 3 below:

Table 2: Inclusion criteria for data gathering

Inclusion criteria	Inclusion reasons
Cases of cyber-attack incidents targeted at healthcare institutions.	Focusing on the healthcare sector makes it very relevant to the subject of study.
Cases of cyber-attacks were reported between 2012 and 2023	This then limits the time range to 2012-2023, which gives a clear window for data collection.
Incidents, which caused disruption of health services, economic loss or system/data compromise, and or litigation.	Inclusion of incidence of cyber-attack with noticeable effects serves to establish the severity of the cyber-attack.
Cases of cyber-attack with credible sources of information and verifiable details	This implies that verifiable information and facts from reliable sources extend the integrity of our work.

Table 3: Exclusion criteria for data gathering

Exclusion criteria	Exclusion reasons
Excluded, therefore, are incidents of cyber-attacks from sectors other than health care.	Research focus is always maintained by excluding incidents of cyber-attacks in the non-healthcare sector.
Exclusion of cyber-attack incidents with insufficient or unverifiable information.	Removal of cyber-attack incidents with insufficient and unverifiable information ascertains quality of the data.
Exclusion of incidents unrelated to cyber-attacks.	The exclusion of non-cyber-attack-related incidents will retain the significance of our research objectives.
Speculative or hearsay cyber-attack incidents ruled out.	Speculative cyber-attack incidents were avoided to maintain the integrity of the research.

Data Sources

To demonstrate justification of the information provided in this paper, all the explored databases are listed below, with majority of the information being extracted from blogs and news media sources. This further stresses the dare need to document and archive all attacks that are experienced by healthcare institutions

- University of Maryland CISSM (Center for International and Security Studies at Maryland)
- U.S. Department of Health and Human Services Office for Civil Rights.
- European Repository of Cyber Incidents (EuRepoC).
- CyberPeace Institute
- The HIPAA (Health Insurance Portability and Accountability Act) Journal.
- Academic journals
- News/media outlets (online)
- Webber Insurance Services
- Blogs

Cyber-Attack Incidents on Healthcare Sector

In the digital age of electronically stored personal information relating to patients' identities, healthcare institutions are beginning to be targeted by cyber attackers. These attacks risk not only patient privacy and safety but also the overall integrity of healthcare systems. Exploring and delineating the trend of cyber-attacks on the healthcare sector is crucial for improving the overall cybersecurity posture of healthcare institutions, protecting patient data, and ensuring the continuity of critical healthcare services in the face of evolving cyber threats. We need to unravel the various types and trends of cyber-attacks on the healthcare sectors because this will increase threat intelligence competencies, improved risk assessment, designing good incident response plan, cyber-attacks trend analysis, information sharing and collaboration among the healthcare sectors. Our findings contains past incidents of cyber-attacks on the healthcare sector.

In the findings (Table 4), we documented some significant cyber-attack incidents that have happened in the healthcare sectors globally from 2012 to 2023, which amounted to 200 attacks incidents in healthcare institutions.

Having a record of previous incidents regarding cyber-attacks against healthcare institutions reveals the common types of cyber-attacks that are widely deployed on healthcare sectors. With such information available, cybersecurity personnel/experts in these institutions can brace themselves and build stronger defenses before an attack strikes. The information will be useful for sharing when there is the need to partner and collaboratively work with stakeholders within the healthcare industry.

Since our paper is primarily centered on analyzing and establishing the trends of cyber-attacks on health institutions, the entire data of cyber-attacks retrieved from the various reports, blog-posts and research papers are not included in this paper, only a snippet of the reports are presented, however, the complete data can be accessed on through the link (https://tinyurl.com/2v5v4977). This link is a repository of the cyber-attacks and the references of where they have been retrieved.

Table 4: Some past cyber-attack incidents on healthcare sector

Authors	Entity targeted	Attack type	Year of attack	Country	Number of individuals affected	Attack source	Impacts of the attack	Response/ mitigation measures
Davis, 2017; Taylor, 2017	ABCD Children's Pediatrics	Ransomware	2017	United States	55,447	Unspecified	Patients Protected Health Information (PHI) compromised. Data encrypted.	ABCD alerted the FBI for the investigation of the cyber incident. Affected patients notified about the attack. Organization cybersecurity enhanced to prevent a future incident. Affected patients were offered one year of free credit monitoring. Breach report submitted to The HHS' Office for Civil Rights.
The HIPAA Journal; McKeon, 2021; Davis, 2022	St. Joseph's/Candler Health System	Ransomware	2021	United States	1,400,000	Unspecified	Patients' data breached. Files encrypted. Lawsuits were filed against St. Joseph's/ Candler (SJ/C).	Systems isolated, staff switched to paper and pen to record patients data, emergency protocols were implemented, law enforcement agencies were notified, investigation was launched.

The HIPAA Journal; Davis, 2019; Terhune, 2015; Vinton, 2015	Perlroth, 2014; Ragan, 2014	Reddy *et al.* (2023)	Revenue Cycle Advisor, 2020; Reddy *et al.* (2023)	Reddy *et al.* (2023); Gatlan, 2020; McGee, 2020	McKeon, 2023; The HIPAA Journal	Reddy *et al.* (2023); Trinity Health, 2020
The University of California, Los Angeles Health System (UCLA)	Community Health Systems	Health Share of Oregon	Florida Orthopaedic Institute	Magellan Health, Inc.	McPherson Hospital	Trinity Health
Unauthorized access/ Disclosure	Hacking/IT incident	Unauthorized access/Disclosure	Ransomware	Ransomware	Ransomware	Ransomware
2015	2014	2019	2020	2020	2022	2020
United States	United States	United States	United States	United States	United States	United States
4,500,000	4,500,000	654,362	640,000	1,013,956	19,020	3,320,726
Unspecified	China hackers	Unspecified	Unspecified	Unspecified	Unspecified	Unspecified
Patients and hospital staff personal information compromised, the impacted patients launched lawsuit against UCLA.	Theft of patients' personal data.	Patients personal and health data exposed.	Data stored on its servers encrypted by the attackers, patients' data breached, lawsuit of $99 million against them.	Patients' data compromised data theft.	Some individuals Protected Health Information (PHI) exposed.	Patients' data and donor information were breached. Files encrypted.
Affected individuals notified, Computer forensic experts were hired to further secure UCLA network, UCLA offered free credit monitoring and $1 million insurance reimbursement policy to those impacted, UCLA agreed to update its cybersecurity practices and policies.	Affected patients notified, identity protection services offered, Agencies under the Health Insurance Portability and Accountability Acts were notified, forensics analysis of the attack was conducted.	Individual affected was notified, vendor security audit program expanded, training policies enhanced. A year free credit monitoring given to affected individuals	Steps to restore impacted data were taken immediately, the environment was secured, internal investigation was initiated, and notifications were sent to affected individuals.	Immediate investigation, Incident reported to law enforcement authorities.	Cybersecurity experts hired to investigate the data breach to determine the extent of the attack. Affected individuals notified of the attack. Complimentary single-bureau credit monitoring services offered to the affected individuals.	Immediate investigation to check if any sensitive information was compromised, potentially impacted patients notified, Federal and State regulatory agencies notified, and attackers were logged out.

The HIPAA Journal	Walker, 2018	Eddie, 2018; Goud, 2018	The HIPAA Journal	The HIPAA Journal; Geer, 2021; Rosenfeld, 2021; Roberts, 2015; Antony *et al.* (2023)	McGee, 2016; The HIPAA Journal; Mangan, 2016; McCann, 2013	Toulas, 2023; The HIPAA Journal
Henwood Family Dentistry	Terros Health	Family Planning NSW	PVHS-ICM Employee Health and Wellness, LLC	Medical Informatics Engineering, Inc. (MIE)	Advocate Health Care	Managed Care of North America (MCNA) Dental
Unauthorized access/ Disclosure	Hacking/IT incident	Ransomware	Ransomware	Unauthorized access/ Disclosure	Unauthorized access/ Disclosure	Ransomware
2023	2018	2018	2017	2015	2013	2023
United States	United States	Australia	United States	United States	United States	United States
7,300	1600	8000	10,143	3,900,000	4,029,530	8,900,000
Unspecified	Unspecified	Unspecified	Unspecified	Unspecified	Unspecified	LockBit ransomware group
Protected health information of patients exposed.	Patients personal information compromised	Clients personal information compromised	Protected Health Information of patients may have been compromised.	Patients' data exposed $100,000 to settle a Health Insurance Portability and Accountability Act (HIPAA) violation connected to a data breach.	Patients' data compromised and exposed, $5.5 Million fine against Advocate Health Care.	Personal data compromised, data theft
Forensic investigation into the attack was done. Federal Bureau of Investigation (FBI) notified about the attack. Affected individuals were offered complimentary credit monitoring and identity theft protection services.	Impacted people informed about the cyber-attack. Internet shut down to contain the attack.	Australian Federal Police was notified of the attack. Website shut down to contain the attack.	Computer expert was hired to conduct forensic investigation of the affected server. Affected individuals notified.	Medical Informatics Engineering contacted its clients to inform them of the data breach, Office for Civil Rights was notified about the breach, the company offered two years of free credit monitoring and identity protection services to all those who were affected.	Letter mailed to affected patients, comprehensive risk analysis and risk management, investigation of the breach, theft reported to law enforcement, new security measures implemented.	Immediate containment of the threat by cybersecurity firm, forensic investigation was done, Law enforcement authorities contacted, notices sent to impacted individuals.

Hutchinson, 2023; The HIPAA Journal	Arghire, 2022; Toulas, 2022; McKeon, 2022	Cheng *et al.* (2017); Mohammed, 2021; Young, 2021; Landi, 2019	Antony *et al.* (2023); Powell, 2023; Southwick, 2023; Ivanova, 2023; Miliard, 2023; Toulas, 2023	Murphy, 2020; Sweny, 2020
Henry Ford Health	Broward Health	Anthem Inc.	HCA Healthcare, Inc.	Northern Light Health
Unauthorized access/Disclosure	Unauthorized access/Disclosure	Hacking/IT incident	Unauthorized access/Disclosure	Ransomware
2023	2021	2015	2023	2020
United States	United States	United States	United States	United States
168, 000	1,357,879	78,800,000	11,000,000	658,000
Unspecified	Unspecified	Chinese national and an unnamed accomplice	Unspecified	Unspecified
Patients' sensitive information exposed.	Patients and employees data was breached, data theft.	Identity theft ,widespread criticism from its members, the media and security experts(Reputational damage), numerous lawsuits against Anthem, significant recovery expenses was incurred after the breach , Anthem agreed to pay $16 million to the Department of Health and Human Services, Office for Civil Rights to settle HIPAA violations.	Personal data of patients stolen, lawsuit against HCA.	Patient information exposed and stolen, financial lost (paid a ransom).
Additional cybersecurity training has been provided to employees. Cybersecurity measures enhanced.	Impacted individual , FBI and the US Department of Justice were notified of the breach, employees advised to change their user passwords, cybersecurity expert contracted to investigate the breach, implementation of multifactor authentication for all users of its systems, two-year membership of identity theft detection and protection was offered to the impacted.	Emails and mails were sent to the affected individuals to notify them of the breach, the company hired cybersecurity firm to look into vulnerabilities of its computer system, and appropriate law enforcement agencies were notified of the breach.	Investigation was launched into the data breach, access to the breached storage location was disabled as an urgent containment measure, the data breach was reported to the relevant authorities, forensic and threat intelligence consultants were engaged in the response and mitigation measures.	Northern Light Health reached out to affected individuals, Federal Department of Health and Human Services was notified of the data breach. Ransom was paid.

The HIPAA Journal	Loyola University Medical Center	Unauthorized access/ Disclosure	2021	United States	16,934	Unspecified	Protected Health Information (PHI) of thousands of patients exposed.	Affected patients notified about the attack. Complimentary membership to a credit monitoring and dark web monitoring service provided for affected individuals for 12 months. More investments in cybersecurity.
Arghire, 2023; Fox, 2023; The HIPAA Journal; Toulas, 2023; Davis, 2023	PharMerica Corporation	Ransomware	2023	United States	5,815,591	Money Message ransomware group	Clients' data compromised and stolen.	Impacted individuals notified of the breach. The organization network was isolated. One year of identity protection fraud monitoring services offered to impacted clients, investigation about the breach was conducted by cybersecurity experts.

RESULTS AND DISCUSSION

In this our research work, we gathered several cyber-attack incidents that happened in the healthcare sector from 2012 to 2023, and we recorded 200 cyber-attack incidents targeted on the Protected Health Information (PHI) of over 256 million individuals. The following analysis and discussion are based on the data gathered in Table 4 above, and the identification of trends in cyber-attacks reveals better understanding of evolving threats in the healthcare sector. Table 5 below shows the number of cyber-attack incidents and total number of individuals affected per year. The highest number of individuals affected was in 2015 with over 108 million people and the highest number of cyber-attacks occurred in 2023, with 71 attacks.

The data in Table 5 above is represented graphically as shown in Figure 2 and Figure 3 below.

Table 5: Cyber-attack incidents and sum of individuals affected per year.

Year	Number of cyber-attack incidents	Total number of individuals affected
2012	1	780,000
2013	2	4,267,993
2014	1	4,500,000
2015	5	108,100,000
2016	2	3,735,000
2017	3	331,713
2018	7	7,129,665
2019	10	2,580,950
2020	19	12,563,390
2021	26	9,469,771
2022	53	34,312,574
2023	71	68,772,064
Total	**200**	**256,543,120**

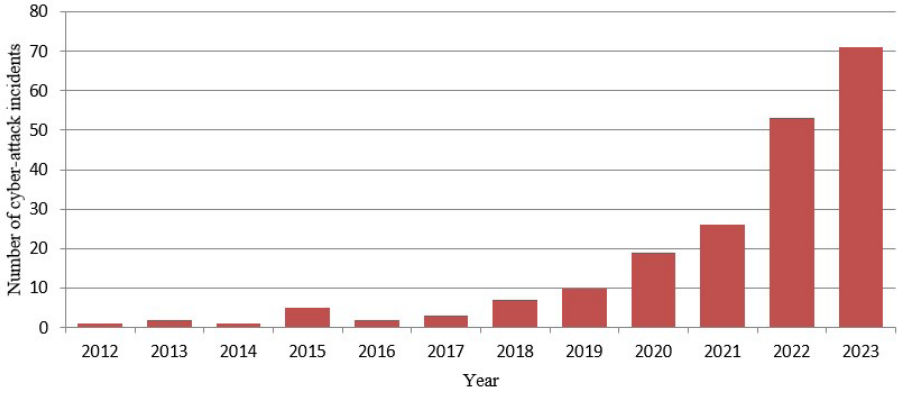

Figure 2: Cyber-attack incidents per year

Figure 2 above shows that there is a significant rise in the number of cyber-attack incidents in the healthcare sector from 2019 to 2023 during and after COVID-19 pandemic.

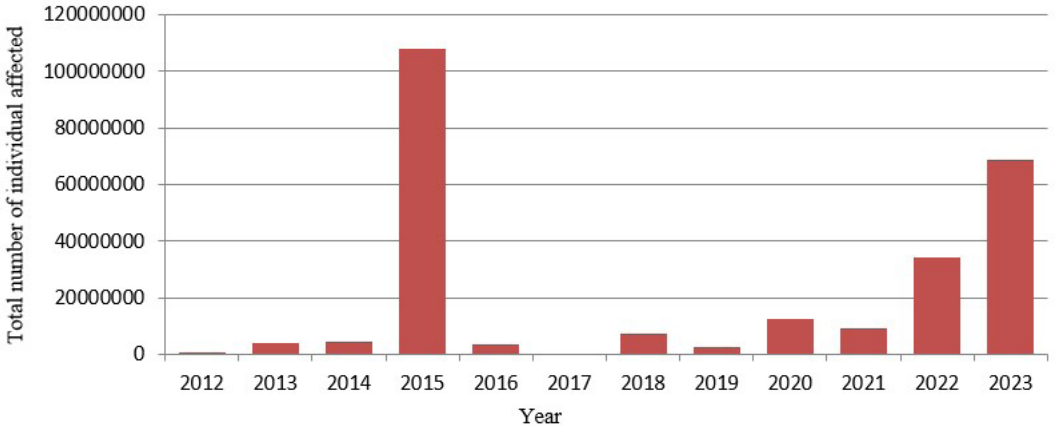

Figure 3: Total number of affected individuals per year.

Figure 3 above shows the total number of individuals affected per year. The total number of affected individuals from 2012 to 2018 was over 128 million, while the total number of affected individuals from the year 2019 to 2023 was over 127 million. From our gathered data, we can see that the total number of affected individuals from 2019 to 2023 was 127,698,749, and that was 6 times of the total number of individuals affected from 2012 to 2018 (20,744,371 million people) with an exclusion of attacks in the year 2015 where over 108 million individuals were affected. The significant rise in the number of cyber-attacks on individual health data in 2015 was a result of a major cyber-attack on the healthcare giant, Anthem Inc. where over 78.8 million individual health data were impacted (Landi, 2019).

Table 6: Geographic distribution of the cyber-attack incidents

Country	Number of cyber-attack incidents
Australia	8
Norway	1
Singapore	2
Thailand	2
United States	174
Ireland	1
Canada	8
Estonia	1
Japan	1
India	1
Hong Kong	1
Total	**200**

We further categorized these attacks geographically to display the most targeted region, however, the data shown (Table 6) is an outcome of documented attacks. Since some countries do not document or provide access to such information.

Most of the incidents happened in the United States, representing either higher incident or more stringent reporting requirements. Other significant incidents were reported in other countries, such as Australia and Canada. In United States, it is mandatory, under Section 13402(e)(4) of the HITECH (Health Information Technology for Economic and Clinical Health) Act, for any healthcare provider, any business associate of that healthcare provider, or health plan to notify the affected individuals, report breaches of unsecured Protected Health Information (PHI) affecting 500 or more individuals to the Secretary of U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) and in some cases to the media (Moffit & Steffen, 2017). Furthermore, we categorized the cyber-attack incidents into 3 categories based on the attack vectors used by the cybercriminals and this is shown in the Table 7 below with the total numbers of individuals affected by each cyber-attack type.

The yearly distribution of cyber-attack type categories is shown in the Table 8 below. The table demonstrates the evolutions of attacks and how outdated cyber-attacks technologies are being used in the modern era to breach systems.

The yearly distribution of attacks has been visualized (Figure 4) to show the trend of the cyber-attack types yearly, and make comparisons on the prominent types deployed towards the health sector. The trend shows that Hacking/IT incident recorded significant rise since 2020, this indicate the most common cyber-attack during and after Covid-19 pandemic. Also, between 2021 and 2022, ransomware attack gained significant rise as most internet fraudsters tend to deploy less popular technologies to attack modern cyber systems, which are not usually anticipated. Contrarily the Unauthorized access/Disclosure has only experienced gradual rise since 2021, but this does not annul the possibility of it being major attack source.

As we can see from our result and discussion, cyber-attacks on healthcare sector is on the rise, and there

Table 7: Cyber-attack types categories

Cyber-attack types	Number of attacks	Total number of individuals affected	% of total number of individuals affected
Unauthorized access/Disclosure	34	39, 562,587	15
Hacking/IT incident	90	145, 714, 273	57
Ransomware	76	71, 266, 260	28
Total	**200**	**256, 543, 120**	**100**

Table 8: Yearly distribution of cyber-attack types categories

Year	Unauthorized access/Disclosure	Hacking/IT incident	Ransomware
2012	0	1	0
2013	1	0	1
2014	0	1	0
2015	2	3	0
2016	0	2	0
2017	0	0	3
2018	3	2	2
2019	2	6	2
2020	4	3	12
2021	3	13	10
2022	8	23	22
2023	11	36	24
Total	**34**	**90**	**76**

is need for healthcare institutions to enhance their cybersecurity practices, this can be achieved by the strong implementation of the following cybersecurity best practices such as;

Regular Risk Assessment

Conducting regular risk assessments will help institutions find potential threats, vulnerabilities; cybersecurity lapses and can also help determine the impact attack can have on the organization (Ataman, 2024; Reddy *et al.*, 2023).

Cybersecurity Training and Awareness

Employers should not assume that their staff members have sufficient technological expertise to identify potential or actual cyber threats .Employees should receive regular training to stay current on security procedures and to emphasize the value of protecting patient privacy. Healthcare institutions can mitigate the possibility of human error resulting in data breaches and foster a culture of security awareness by investing in training for staff (Malecki, 2019; Nidiganti, 2024).

Data Encryption

Transforming confidential and sensitive patient information into a coded language that is only accessible by authorized personnel with a decryption key is known as data encryption in the healthcare industry. Accordingly, even if someone unauthorized have access to the data they will be unable to view or utilize it without the proper key (Ataman, 2024).

Compliance with Regulations

In United States, healthcare institutions are required under the HIPAA (Health Insurance Portability and

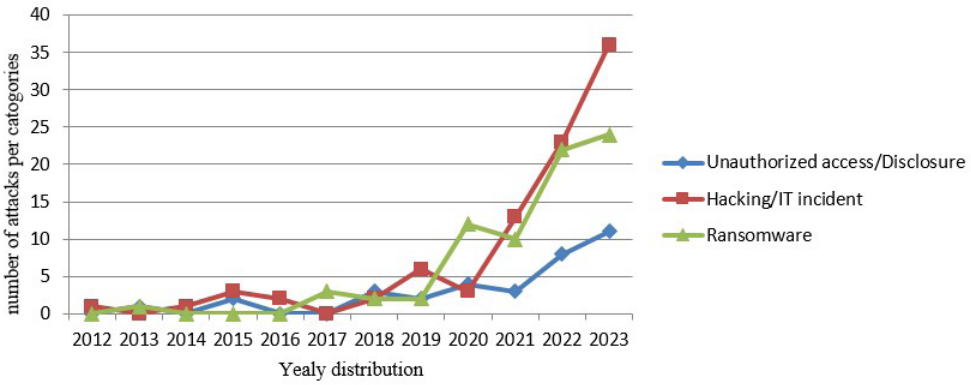

Figure 4: Comparison of the cyber-attack categories yearly distribution

Accountability Act) Security Rule to have measures in place, like encryption, which renders electronic Protected Health Information (ePHI) unusable for cybercriminals. In addition to HIPAA, the Health Information Technology for Economic and Clinical Health Act (HITECH) protects Protected Health Information (PHI) from misuse and unauthorized access. Compliance with regulations will also guarantee the privacy of sensitive medical data (Biswas, 2023; Burns & Johnson, 2015).

Access Control

Implementation of access control such as Multi-factor authentication (MFA) and role-based access controls ensures that only authorized personnel have access to sensitive data and systems. Multi-factor authentication (MFA) provides additional layers of security, so in addition to a simple method of authenticating a user – for example, password – another form of verification is sent to a user's email address or mobile device; an OTP generates a time–based code, meaning at least two factors have been verified (Suleski *et al.*, 2023; Ataman, 2024).

Network Security

The basis of protection for the patient's data lies in network security. It can get any better by the following: implementing firewalls, IPS (Intrusion Prevention Systems), DLP (Data Loss Prevention), SDN (Software-defined Networking), and SD-WAN (Software-defined Wide Area Networks) solutions, and secure communication protocols to protect the organizational network. Network segmentation is one such idea that isolates sensitive data and systems that are to be breached (Biswas, 2023; Aydın *et al.*, 2009).

CONCLUSION

The fast-growing cybersecurity crisis in the healthcare sector requires urgent and collaborative efforts by all parties concerned. This research has pointed out several alarming trends in the incidence of cyber-attacks against healthcare institutions, pointing to significant consequences for patient safety, data integrity, and institutional trust.

In the setting of ever-escalating cyber threats in both sophistication and frequency, embedding cybersecurity into the core of operational policy becomes paramount for healthcare professionals and institutions. Those healthcare providers that adopt a culture of security and invest in appropriate state-of-the-art protective measures are better positioned to mitigate risks and safeguard sensitive patient information, and the overall resilience of the healthcare system. This call to action reminds one that the responsibility to protect healthcare data spans all levels of the organization and requires collaborative efforts to strengthen their defenses against an ever-sophisticating cyber threat landscape.

LIMITATIONS

- Some incidents of cyber-attacks in healthcare institutions are mostly not reported by them due to legal, regulatory, and reputational reasons. Hence, these cases couldn't be covered in our gathered data because of their lack of transparency.
- Reliance on particular sources for collecting data-for instance, news articles or governmental reports-embeds bias into the latter about event types being overrepresented and which ones are not even reported

RECOMMENDATIONS

- Future research study should explore the vulnerabilities in the healthcare sector that are most commonly exploited by cybercriminals.
- Short-term and long-term impacts of cyber-attacks on healthcare institutions, including financial costs and organization reputation damage should be examined.

Acknowledgements

The authors would like to express their gratitude to IMT Mines Ales for providing us with a well conducive environment for our research. Also, we extend our profound gratitude to the Petroleum Technology Development Fund (PTDF), Nigeria for their educational scholarship for author Muritala Kolade Yusuf

REFERENCES

Ahmed, M. M., Maglaras, L., & Ferrag, M. A. (2020). Cyber threats in the healthcare sector and countermeasures. In *Advances in business strategy and competitive advantage* (pp. 109–124). https://doi.org/10.4018/978-1-7998-3648-3.ch007

Al-Qarni, E. A. (2023). Cybersecurity in healthcare: A review of recent attacks and mitigation strategies. *International Journal of Advanced Computer Science and Applications, 14*(5). https://doi.org/10.14569/ijacsa.2023.0140513

Antony, A., Thomas, S., Varghese, T., & Padman, V. (2023, December). *Ransomware attacks on healthcare systems: Case studies and mitigation strategies.* https://www.researchgate.net/publication/376514138_Ransomware_Attacks_on_Healthcare_Systems_Case_Studies_and_Mitigation_Strategies

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J. M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making, 20*(1). https://doi.org/10.1186/s12911-020-01161-7

Arghire, I. (2022, January 5). *Broward Health data breach impacts 1.3 million people.* SecurityWeek. https://www.securityweek.com/broward-health-data-breach-impacts-13-million-people/

Arghire, I. (2023, May 16). *PharMerica discloses data breach impacting 5.8 million individuals.* SecurityWeek. https://www.securityweek.com/pharmerica-discloses-data-breach-impacting-5-8-million-individuals/

Ataman, A. (2024, May 9). *Cybersecurity in healthcare: 7 challenges & 10 best practices in '23*. AIMultiple: High Tech Use Cases & Tools to Grow Your Business. https://research.aimultiple.com/cybersecurity-in-healthcare/

Aydın, M. A., Zaim, A. H., & Ceylan, K. G. (2009). A hybrid intrusion detection system design for computer network security. *Computers & Electrical Engineering, 35*(3), 517–526. https://doi.org/10.1016/j.compeleceng.2008.12.005

Bhosale, K. S., Nenova, M., & Iliev, G. (2021, September). A study of cyber attacks: In the healthcare sector. In *2021 Sixth Junior Conference on Lighting (Lighting)* (pp. 1-6). IEEE. https://doi.org/10.1109/lighting49406.2021.9598947

Biswas, D. (2023, January 10). *Cybersecurity best practices for healthcare you need to know*. AppViewX. https://appviewx.com/blogs/cybersecurity-best-practices-for-healthcare-you-need-to-know/

Burns, A., & Johnson, M. E. (2015). Securing health information. *IT Professional, 17*(1), 23–29. https://doi.org/10.1109/mitp.2015.13

Cheng, L., Liu, F., & Yao, D. D. (2017, June 9). Enterprise data breach: Causes, challenges, prevention, and future directions. *WIREs Data Mining and Knowledge Discovery, 7*(5). https://doi.org/10.1002/widm.1211

CyberPeace Institute. (n.d.). *Cyber attacks in times of conflict*. CyberPeace Institute. https://cyberconflicts.cyberpeaceinstitute.org/

Davis, J. (2017, April 5). *Ransomware attack on Texas pediatric provider exposes data of 55,000 patients*. Healthcare IT News. https://www.healthcareitnews.com/news/ransomware-attack-texas-pediatric-provider-exposes-data-55000-patients

Davis, J. (2019, March 21). *UCLA Health reaches $7.5M settlement over 2015 breach of 4.5M*. HealthITSecurity. https://healthitsecurity.com/news/ucla-health-reaches-7.5m-settlement-over-2015-breach-of-4.5m

Davis, J. (2022, June 23). *10 biggest healthcare data breaches of 2021 impact over 22.6M patients*. SC Media. https://www.scmagazine.com/feature/10-biggest-healthcare-data-breaches-of-2021-impact-over-22-6m-patients

Davis, J. (2023, May 15). *Data of 5.82M PharMerica patients stolen, accessed during cyberattack*. SC Media. https://www.scmagazine.com/news/5-82m-pharmerica-patients-stolen-accessed-cyberattack

Eddie, R. (2018, May 15). *Cyber attack compromises patient information at Family Planning NSW*. The New Daily. https://www.thenewdaily.com.au/news/state/nsw/2018/05/14/family-planning-nsw-cyber-attack

EuRepoC: European Repository of Cyber Incidents. (2024, April 22). *EuRepoC*. https://eurepoc.eu/

Fox, A. (2023, May 16). *PharMerica announces health data breach, possibly largest of Q1 2023*. Healthcare IT News. https://www.healthcareitnews.com/news/pharmerica-announces-health-data-breach-possibly-largest-q1-2023

Gatlan, S. (2020, May 13). *Healthcare giant Magellan Health hit by ransomware attack*. BleepingComputer. https://www.bleepingcomputer.com/news/security/healthcare-giant-magellan-health-hit-by-ransomware-attack/

Geer, D. (2021, December 7). *Medical Informatics Engineering breach: The gift that keeps on giving*. Medium. https://medium.com/the-aftermath-of-a-data-breach/medical-informatics-engineering-breach-the-gift-that-keeps-on-giving-9948231d2e95

Goud, N. (2018, May 14). *Ransomware attack on Family Planning NSW*. Cybersecurity Insiders. https://www.cybersecurity-insiders.com/ransomware-attack-on-family-planning-nsw/

Haleem, A., Javaid, M., Singh, R. P., & Suman, R. (2021). Telemedicine for healthcare: Capabilities, features, barriers, and applications. *Sensors International, 2*, 100117. https://doi.org/10.1016/j.sintl.2021.100117

Hutchinson, D. (2023, July 17). *Henry Ford Health confirms data breach affecting 168,000 patients*. WDIV. https://www.clickondetroit.com/news/local/2023/07/17/henry-ford-health-confirms-data-breach-affecting-168000-patients/

Ivanova, I. (2023, July 11). *HCA Healthcare says hackers stole data on 11 million patients*. CBS News. https://www.cbsnews.com/news/hca-healthcare-data-breach-hack-11-million-patients-affected/

Kale, B., Aworo, S., & Anyangwu, C. (2022). *Cyber-attacks on digital infrastructures in healthcare: The secured approach*. ResearchGate. https://www.researchgate.net/publication/366323639_Cyber-Attacks_on_Digital_Infrastructures_in_HealthCare_The_Secured_Approach

Lagasse, J. (2020, September 9). *Personal information of 348,000 people potentially exposed in NorthShore data breach*. Healthcare Finance News. https://www.healthcarefinancenews.com/news/personal-information-348000-people-potentially-exposed-northshore-data-breach

Landi, H. (2019, May 10). *DOJ charges Chinese national, accomplice in landmark Anthem hack*. Fierce Healthcare. https://www.fiercehealthcare.com/payer/doj-charges-chinese-national-accomplice-landmark-anthem-hack

Mahmood, G. S., Huang, D. J., & Jaleel, B. A. (2019). A secure cloud computing system by using encryption and access control model. *Journal of Information Processing Systems, 15*(3), 538–549. https://doi.org/10.3745/jips.03.0117

Mahmoud, R., & Al-Najjar, Y. (2024). *Cybersecurity in healthcare industry*. ResearchGate. https://www.researchgate.net/publication/378480107_CYBERSECURITY_IN_HEALTHCARE_INDUSTRY

Malecki, F. (2019). Best practices for preventing and recovering from a ransomware attack. *Computer Fraud & Security, 2019*(3), 8–10. https://doi.org/10.1016/s1361-3723(19)30028-4

Mangan, D. (2016, August 5). *Huge data breach at health*

system leads to biggest ever settlement. CNBC. https://www.cnbc.com/2016/08/04/huge-data-breach-at-health-system-leads-to-biggest-ever-settlement.html

McCann, E. (2013, September 6). *Advocate Health slapped with lawsuit after massive data breach.* Healthcare IT News. https://www.healthcareitnews.com/news/AdvocateHealth-slapped-with-lawsuit-after-massive-data-breach

McGee, M. (2016, August 4). *Advocate Health hit with record $5.5 million HIPAA penalty.* CareersInfoSecurity. https://www.careersinfosecurity.com/advocate-health-hit-record-55-million-hipaa-penalty-a-9307

McGee, M. (2020, October 13). *Health data breaches in 2020: Ransomware incidents dominate.* DataBreachToday. https://www.databreachtoday.com/health-data-breaches-in-2020-ransomware-incidents-dominate-a-15170

McKeon, J. (2021, September 20). *St. Joseph's/Candler faces lawsuits in wake of ransomware attack.* HealthITSecurity. https://healthitsecurity.com/news/st-josephs-candler-faces-lawsuits-in-wake-of-ransomware-attack

McKeon, J. (2022, January 4). *PHI breach, data exfiltration at Broward Health impacts 1.3 million.* HealthITSecurity. https://healthitsecurity.com/news/phi-breach-data-exfiltration-at-broward-health-impacts-1.3-million

McKeon, J. (2023, May 10). *Healthcare data breach at Kansas hospital impacts 19K.* HealthITSecurity. https://healthitsecurity.com/news/healthcare-data-breach-at-kansas-hospital-impacts-19k

Meadows, J. (2020, September 9). *Ransomware attack exposes NorthShore, Northwestern patient data.* Evanston, IL Patch. https://patch.com/illinois/evanston/ransomware-attack-exposes-northshore-northwestern-patient-data

Meisner, M. (2018). Financial consequences of cyber attacks leading to data breaches in healthcare sector. *Copernican Journal of Finance & Accounting, 6*(3), 63. https://doi.org/10.12775/cjfa.2017.017

Miliard, M. (2023, July 18). *HCA Healthcare sued for recent data breach.* Healthcare IT News. https://www.healthcareitnews.com/news/hca-healthcare-sued-recent-data-breach

Moffit, R., & Steffen, B. (2017, June). *Health care data breaches: A changing landscape.* Maryland Health Care Commission. https://mhcc.maryland.gov/mhcc/pages/hit/hit/documents/HIT_DataBreachesBrief_Brf_Rpt_090717.pdf

Mohammed, Z. A. (2021, November 9). *Data breach recovery areas: An exploration of organization's recovery strategies for surviving data breaches. Organizational Cybersecurity Journal.* https://doi.org/10.1108/ocj-05-2021-0014

Moore, W., & Frye, S. (2019). Review of HIPAA, Part 1: History, protected health information, and privacy and security rules. *Journal of Nuclear Medicine Technology, 47*(4), 269–272. https://doi.org/10.2967/jnmt.119.227819

Murphy, D. (2020, September 16). *Northern Light Health caught up in data breach.* Press Herald. https://www.pressherald.com/2020/09/15/northern-light-health-informs-public-of-data-breach/

Nidiganti, V. (2024, March 25). *Best practices for healthcare cybersecurity.* Rely Services Inc. https://www.relyservices.com/blog/healthcare-cybersecurity-best-practices

Perlroth, N. (2014, August 19). *Hack of Community Health Systems affects 4.5 million patients.* Bits Blog. https://archive.nytimes.com/bits.blogs.nytimes.com/2014/08/18/hack-of-community-health-systems-affects-4-5-million-patients/

Powell, O. (2023, July 19). *HCA Healthcare data breach impacts 11 million.* Cybersecurity Hub. https://www.cshub.com/attacks/news/hca-healthcare-data-breach-impacts-11-million-patients

Ragan, S. (2014, August 18). *Community Health Systems blames China for recent data breach.* CSO Online. https://www.csoonline.com/article/548106/data-protection-community-health-systems-blames-china-for-recent-data-breach.html

Reddy, J., Elsayed, N., ElSayed, Z., & Ozer, M. (2023, February 22). A review on data breaches in healthcare security systems. *International Journal of Computer Applications, 184*(45), 1–7. https://doi.org/10.5120/ijca2023922333

Revenue Cycle Advisor. (2020, July 21). *Florida Orthopaedic Institute reports breach affecting 640K individuals.* HealthLeaders Media. https://www.healthleadersmedia.com/innovation/florida-orthopaedic-institute-reports-breach-affecting-640k-individuals

Roberts, P. (2015, July 31). *4.5 million doctors still in the dark after electronics records hack exposes data on 4 million.* The Security Ledger With Paul F. Roberts. https://securityledger.com/2015/07/doctors-still-in-the-dark-after-electronics-records-hack-exposes-data-on-4-million/

Rosenfeld, S. (2021, February 14). *Medical Informatics Engineering pays $100K for data breach of 3.5M patients.* OncLive. https://www.chiefhealthcareexecutive.com/view/medical-informatics-engineering-pays-100k-for-data-breach-of-35m-patients

Schencker, L. (2020, September 9). *NorthShore health system says personal information of 348,000 people potentially exposed in data breach.* Chicago Tribune. https://www.chicagotribune.com/2020/09/08/northshore-health-system-says-personal-information-of-348000-people-potentially-exposed-in-data-breach/

Senbekov, M., Saliev, T., Bukeyeva, Z., Almabayeva, A., Zhanaliyeva, M., Aitenova, N., Toishibekov, Y., & Fakhradiyev, I. (2020). The recent progress and applications of digital technologies in healthcare: A review. *International Journal of Telemedicine and Applications, 2020,* 1–18. https://doi.org/10.1155/2020/8830200

Southwick, R. (2023, July 10). *HCA Healthcare discloses data breach affecting as many as 11 million patients.* OncLive. https://www.chiefhealthcareexecutive.com/view/hca-healthcare-discloses-data-breach-affecting-as-

many-as-11-million-patients

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). *A review of multi-factor authentication in the Internet of Healthcare Things. Digital Health, 9,* 205520762311771. https://doi.org/10.1177/20552076231177144

Swasey, K. (2020, April). *Insufficient healthcare cybersecurity invites ransomware attacks and sale of PHI on the dark web.* https://www.usu.edu/cai/files/studentpaper-swasey.pdf

Sweny, G. (2020, September 14). *Millions of individuals fall victim to cyberattacks on healthcare institutions.* AgileBlue. https://agileblue.com/millions-of-individuals-fall-victim-to-cyberattacks-on-healthcare-institutions/

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2022). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security, 12*(3). https://doi.org/10.17762/ijcnis.v12i3.4817

Taylor, E. (2017, August 16). *ABCD Pediatrics hit by ransomware attack affecting 55,000 patients.* Defensorum. https://www.defensorum.com/abcd-pediatrics-hit-ransomware-attack-affecting-55000-patients/

Terhune, C. (2015, July 18). *UCLA Health System data breach affects 4.5 million patients.* Los Angeles Times. https://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html

The HIPAA Journal - news and articles about HIPAA. (n.d.). https://www.hipaajournal.com/

Tin, D., Hata, R., Granholm, F., Ciottone, R. G., Staynings, R., & Ciottone, G. R. (2023). Cyberthreats: A primer for healthcare professionals. *The American Journal of Emergency Medicine, 68,* 179–185. https://doi.org/10.1016/j.ajem.2023.04.001

Toulas, B. (2022, January 3). *Broward Health discloses data breach affecting 1.3 million people.* BleepingComputer. https://www.bleepingcomputer.com/news/security/broward-health-discloses-data-breach-affecting-13-million-people/

Toulas, B. (2023, May 15). *Ransomware gang steals data of 5.8 million PharMerica patients.* BleepingComputer. https://www.bleepingcomputer.com/news/security/ransomware-gang-steals-data-of-58-million-pharmerica-patients/

Toulas, B. (2023, May 29). *MCNA Dental data breach impacts 8.9 million people after ransomware attack.* BleepingComputer. https://www.bleepingcomputer.com/news/security/mcna-dental-data-breach-impacts-89-million-people-after-ransomware-attack/

Toulas, B. (2023, July 11). *HCA confirms breach after hacker steals data of 11 million patients.* BleepingComputer. https://www.bleepingcomputer.com/news/security/hca-confirms-breach-after-hacker-steals-data-of-11-million-patients/

Trinity Health's response to the Blackbaud philanthropy database security incident. (2020, September 15). *Trinity Health's Response to the Blackbaud Philanthropy Database Security Incident.* PR Newswire. https://www.prnewswire.com/news-releases/trinity-healths-response-to-the-blackbaud-philanthropy-database-security-incident-301130466.html

University of Maryland CISSM Cyber Attacks Database. (n.d.). *Cyber attacks database.* https://cissm.liquifiedapps.com/

U.S. Department of Health & Human Services - Office for Civil Rights. (n.d.). *Breach portal.* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Vinton, K. (2015, July 18). *4.5 million UCLA Health patients' data compromised in cyber attack.* Forbes. https://www.forbes.com/sites/katevinton/2015/07/17/4-5-million-ucla-health-patients-data-compromised-in-cyber-attack/?sh=4a5a1ae42bc6

Webber Insurance Services. (2024, August 29). *List of data breaches and cyber attacks in Australia 2018-2024.* https://www.webberinsurance.com.au/data-breaches-list

Walker, M. (2018, June 10). T*erros Health data breach potentially impacts 1,600 patients.* ABC15 Arizona in Phoenix (KNXV). https://www.abc15.com/news/region-phoenix-metro/central-phoenix/terros-health-data-breach-1600-patients-potentially-impacted

Yeng, P., Fauzi, M. A., Yang, B., Diekuu, J. B., Nimbe, P., Holik, F., ... & Sun, L. (2023, October). SecHealth: Enhancing EHR Security in digital health transformation. In *Proceedings of the 8th International Conference on Sustainable Information Engineering and Technology* (pp. 538-544). https://doi.org/10.1145/3626641.3627214

Young, K. (2021, November 1). *Cyber case study: Anthem data breach.* CoverLink Insurance - Ohio Insurance Agency. https://coverlink.com/case-study/anthem-data-breach/