Global Scientific JOURNALS

GSJ: Volume 12, Issue 2, February 2024, Online: ISSN 2320-9186
www.globalscientificjournal.com

CYBERSECURITY IN HEALTHCARE INDUSTRY

Raghad Mahmoud, Yusra Al Najjar

Raghad Mahmoud, Medical Analysis, Al Balqua'a Applied University, Jordan, E-mail: raghad.abed.borini@gmail.com
Yusra AL Najjar, Assistant Professor, Computer and Information Technology, Taibah University, KSA, E-mail: yalnajar@taibahu.edu.sa

Keywords
Cybersecurity; cyber-attack; healthcare; threats; attackers; vulnerability breaches.

ABSTRACT

Ensuring the security of health information has started as a significant obligation for healthcare organizations across the board. While medical equipment and applications are crucial to patient care, they have also become main targets for malicious actors. Attackers illegally target healthcare data, often aiming to install ransomware software once they breach the network, they lock and encrypt data until a ransom is paid. Consequently, organizations often find themselves forced to pay large amounts to regain access to and decrypt their data. While the theft of healthcare equipment may be less publicized, attackers may steal network-connected equipment for alternative purposes. Thus, there is an urgent need to implement robust cybersecurity measures within the healthcare sector to safeguard all information. Breaches in information security can be accomplished through various passages, including laboratory and hospital records, insurance documentation, and physical records, as well as electronic medical records and tracking systems. Cybersecurity measures can effectively protect these records against unauthorized access. This paper demonstrates different types of cybercrimes that occur in medical information and strategies to mitigate them, shedding light on numerous cybercrimes that have occurred over the past decade and what should be done to mitigate these crimes. Given the value of healthcare information, it has become a profitable target for cybercriminals.

1. INTRODUCTION

Cybersecurity holds an exceptional level of importance within medical organizations today. From health departments to care providers, diagnostic services to research institutions, and primary healthcare practices, are areas that are susceptible to data theft, data breaches, and systems being held hostage for ransom. By deploying robust security protocols that integrate advanced authentication methods alongside thorough staff training organizations can significantly mitigate the risk of breaches and the subsequent potential cyber threats. Particularly vulnerable to cyberattacks is a specific aspect of healthcare, often targeted by hackers to exploit vulnerabilities within an organization's supply chain (Jeff Tully, 2020) (Wong, 2014).

Knowing that hackers often maintain a step ahead of corporations sets one of the greatest challenges in the field of cybersecurity. Hackers always seek out security vulnerabilities that may be unseen or ignored by individuals within the organization. Moreover, the rapid evolution of new technologies, particularly in cloud computing and mobile applications, proceeds at an exponential pace. Hackers swiftly adapt to employ these emerging technologies to their advantage, necessitating cybersecurity specialists to remain cautious and predict and prevent their efforts. Many security solutions primarily focus on identifying malware and preventing unauthorized access. Consequently, rather than taking proactive measures, organizations often find themselves reacting to current and potential threats (Kinross, 2017).

2. CYBERSECURITY IN HEALTHCARE

Healthcare providers may be involved with suppliers without conducting a prior risk assessment. For instance, hospital staff may gain computer access when the facility contracts a cleaning company. While safeguarding patient information from ordinary employees is crucial, it can be challenging due to the essential nature of maintenance and cleaning for a safe work environment. Upgrading to a new system incurs costs such as technician wages and acquiring new technology, which may also result in downtime, thereby reducing the hospital's revenue-generating capacity. Moreover, obtaining certification for new technology and equipment can be time-consuming (Suman, 2021).

The healthcare sector should prioritize data security and consider the implications of the information collected during medical treatments. However, the sector faces challenges due to the multitude of entry and access points, making it difficult for a single entity to establish an effective data security system. Profile-based secure access to business applications and data is necessary for the healthcare industry (Aaron Turransky, 2022).

3. Harmful Threats of Cybersecurity in Healthcare

To implement cybersecurity properly on the organizational level, it is not enough to establish a department that is responsible for cybersecurity and asset management, it should also include comprehensive cooperation between different fields in the cybersecurity industry and follow a pre-active approach for creating responses for newly developed cyber-attacks. Cyber-attacks in healthcare organizations can be classified that differ according to exploited system vulnerabilities, their proportional impacts, and protection strategies (Services, 2023).

3.1 E-mail phishing attach

To modify the running headings, select View | Header and Footer. Click inside the text box to type the name of the journal the article is being submitted to and the manuscript identification number. Click the forward arrow in the pop-up toolbar to modify the header or footer on subsequent pages.

3.2 The ransomware attack

This type of malicious software (malware) involves encryption of data. It is easily installed and frequently reaches devices through phishing emails containing malicious files or links. Installing email gateway security and educating users about best practices for email security is recommended. Attackers started increasingly targeting victims' backups to prevent organizations from restoring their data. Veeam's "2023 Ransomware Trends Report" found more than 93% of ransomware attacks the previous year specifically targeted backup data (Irei, n.d.).

3.3 Breach of Data

Data breaching involves the unauthorized distribution of sensitive information intended to remain confidential. This occurs when data is disclosed to unsecured channels either intentionally or unintentionally. It happens when a third party or unauthorized individual attempts to steal or access data, which may include trade secrets, company shares, transaction details, or legal information. Various types of data breaches include phishing, denial of service attacks, malware, and exfiltration.

Data breaches may not always result from inherent risks, although they can occur when malware, compromised company emails, or insider attacks are factors. Given the significant demand for health information among financially motivated criminals, the healthcare sector is frequently targeted. It is recommended to implement data encryption and data backup measures (US health insurer Anthem hit by massive data breach).

3.4 Unsecured medical equipment

In the contemporary era, hospitals store a substantial volume of medical data. Linked medical equipment is indispensable for treating patients across all healthcare providers. Due to their frequent utilization, ensuring secure access to these medical tools and equipment is paramount. Regrettably, many hospitals do not prioritize this aspect adequately, increasing the risk of a significant cyberattack. The attack on connected medical devices may affect patient safety (Ekaterina Balandina, 2015).

3.5 Lack of security awareness

When users are unaware of security best practices, they are less inclined to adhere to security policies and behave securely. This increases the risk of cybersecurity in healthcare facilities. Consequently, healthcare institutions, serving as the last line of defense, may be particularly susceptible to external threats. Strengthening defenses requires a combination of technical investments and security awareness initiatives (Kim, 2017).

3.6 Vulnerability of old systems

Replacing outdated systems with modernized ecology is essential for progress. However, many healthcare institutions are reluctant to embrace change and let go of their established practices. This hesitancy increases the risk of significant cyberattacks, as outdated systems lack protection against current viruses and malware. Insufficient funding, the cost of training employees, regulatory obligations, and complacency are factors necessitating the upgrade of IT infrastructure, thereby leaving vulnerabilities open to exploitation by cybercriminals.

Apart from cyber threats, the risk of physical theft looms large within organizations, as it may involve the theft of backup tapes, and systems containing sensitive healthcare records from within the organization. Moreover, unauthorized duplication of data using backup tools like flash memory may also happen (Steven Furnell, 2001).

The following section shows the biggest data breaches that occurred in the healthcare field.

4. Biggest Healthcare Data Breaches

The healthcare industry encounters numerous data breaches. In this segment, we present several cases that occurred in the previous decade. Table 2 illustrates the incidents, including the timing, impact, targeted data, and recommended response plan.

Table 2: The biggest data breaches in healthcare ranked by impact (Kot, 2024)

Event	Date	Impact	How did the breach occur?	What data was compromised?	Lesson learned
Tricare Data Breach	Sept. 2011	5 million patients	backup tapes theft of healthcare records	Social security numbers, names, addresses, phone numbers, personal health data, clinical notes, lab tests, and prescription information	A data encryption policy compliant with federal standards should be put into effect.
Community Health Systems Data Breach	Apr.-June 2014	4.5 million patients	Exploiting a software vulnerability by deploying a highly sophisticated malware	Names, birth dates, social security numbers, phone numbers, and addresses	Employees should be made aware of the indicators signaling attempts to inject malware and other threats, address vulnerabilities, and consult the CVE database to stay updated on zero-day exploits.
UCLA Health Data Breach	July 2015	4.5 million patients	Cyber-attack compromised sensitive patient information	Names, Data of birth, social security numbers, Medicaid, Health plan identification numbers, and some medical data	Ensure a thorough investigation is undertaken upon the discovery of any suspicious activity.
Advocate Health Care Data Breach	Aug. 2013	4.03 million patients	Theft of four personal computers storing unencrypted medical information	Names, addresses, birth dates, credit card numbers, demographic info, clinical info, and health insurance info	physical security control, and encryption practices should be implemented.
Medical Informatics Engineering Data Breach	July 2015	3.9 million patients	access to MIE's servers using uncompromised usernames and passwords	Names, telephone numbers, mail addresses, usernames, hashed passwords, security questions and answers, spousal info, email addresses, birth dates, SSN, lab results, health insurance policy info, diagnosis, disability codes doctor names, medical conditions, names of children, and birth statistics	Dark web monitoring solution.
Newkirk Products Data Breach	July 2016	3.8 million patients	Unauthorized access to servers	Primary care provider information, medical ID numbers, patient and dependents names, birth dates, and invoice information	Regularly test server software for security vulnerabilities and misconfigurations, consistently scan servers for potential exploits, and safeguard all privileged access management.
Banner Health Data Breach	Aug. 2016	3.62 million patients	Unauthorized access to a private server	Names, addresses, birth dates, SSN, appointment dates, physician, and health insurance information	Verify third-party vendors' adherence to mandatory financial regulations and continually enhance security postures.
Trinity Health Data Breach	May 2020	3.3 million patients	Ransomware attack, hackers exfiltrated data	Names, addresses, birth dates, healthcare providers, services data, medical num-	Deploy a third-party vendor attack surface monitoring solution and refuse to com-

				bers, immunization types, lab results, medications, claim and financial information	ply with cybercriminal demands under any circumstances.
Shields Healthcare Group Data Breach	Mar.2022	2 million people	Unauthorized access to a network server	Names, birth dates, addresses, provider, diagnosis and billing information, insurance numbers, medical record numbers, patient IDs	Zero-trust approach.
Broward Health Data Breach	Jan. 2022	1.3 million patients	Breach through a compromised third-party medical provider	Names, addresses, birth dates, driver's license numbers, insurance, and medical information	Enforce multi-factor authentication for accessing all endpoints, ensure secure privileged access management, and monitor all connections to endpoints diligently.
Morley Companies Data Breach	Feb. 2022	521,046 individuals	Ransomware attack	Names, addresses, SSN, birth dates, client ID numbers, medical diagnosis and treatment information, and health insurance information	The delay in notification heightened the risk of breaching the HIPSS Breach Notification rule; notifications should be made promptly and directly.
L'Assurance Maladie Data Breach	Mar.2022	510,000 people	Retrieving the passwords for 19 accounts belonging to pharmacists from the dark web	Names, surnames, dates of birth, SSN, GP details, and level of reimbursement	Deploy multi-factor authentication and implement a data leak detection solution.
ARcare Data Breach	Feb. 2022	345,000 people	Maintaining unauthorized access inside computer systems, exposing on the internet, and stealing sensitive data for ransom	Names, SSN, driver's license numbers, state identification numbers, dates of birth, financial account information, medical treatment information, prescription information, medical diagnosis information, condition information, and health insurance information	Evaluate data security practices and explore advanced risk mitigation strategies.
OneTouchPoint (OTP)	July 2022	2.6 million people	Locking and encrypting files	Names, addresses, birthdays, medical records, patient demographics, employment dates and ID numbers, service descriptions and dates, test results, and diagnosis codes	Annual review of security policies.
Event	Date	Impact	How did the breach occur?	What data was compromised?	Lesson learned
Tricare Data Breach	Sept. 2011	5 million patients	backup tapes theft of healthcare records	Social security numbers, names, addresses, phone numbers, personal health data, clinical notes, lab tests, and prescription information	A data encryption policy compliant with federal standards should be put into effect.
Community Health Systems Data Breach	Apr.-June 2014	4.5 million patients	Exploiting a software vulnerability by deploying a highly sophisticated malware	Names, birth dates, social security numbers, phone numbers, and addresses	Employees should be made aware of the indicators signaling attempts to inject malware and other threats, address vulnerabilities, and consult the CVE database to stay updated on zero-day

					exploits.
UCLA Health Data Breach	July 2015	4.5 million patients	Cyber-attack compromised sensitive patient information	Names, Data of birth, social security numbers, Medicaid, Health plan identification numbers, and some medical data	Ensure a thorough investigation is undertaken upon the discovery of any suspicious activity.
Advocate Health Care Data Breach	Aug. 2013	4.03 million patients	Theft of four personal computers storing unencrypted medical information	Names, addresses, birth dates, credit card numbers, demographic info, clinical info, and health insurance info	physical security control, and encryption practices should be implemented.
Medical Informatics Engineering Data Breach	July 2015	3.9 million patients	access to MIE's servers using uncompromised usernames and passwords	Names, telephone numbers, mail addresses, usernames, hashed passwords, security questions and answers, spousal info, email addresses, birth dates, SSN, lab results, health insurance policy info, diagnosis, disability codes doctor names, medical conditions, names of children, and birth statistics	Dark web monitoring solution.
Newkirk Products Data Breach	July 2016	3.8 million patients	Unauthorized access to servers	Primary care provider information, medical ID numbers, patient and dependents names, birth dates, and invoice information	Regularly test server software for security vulnerabilities and misconfigurations, consistently scan servers for potential exploits, and safeguard all privileged access management.
Banner Health Data Breach	Aug. 2016	3.62 million patients	Unauthorized access to a private server	Names, addresses, birth dates, SSN, appointment dates, physician, and health insurance information	Verify third-party vendors' adherence to mandatory financial regulations and continually enhance security postures.
Trinity Health Data Breach	May 2020	3.3 million patients	Ransomware attack, hackers exfiltrated data	Names, addresses, birth dates, healthcare providers, services data, medical numbers, immunization types, lab results, medications, claim and financial information	Deploy a third-party vendor attack surface monitoring solution and refuse to comply with cybercriminal demands under any circumstances.
Shields Healthcare Group Data Breach	Mar.2022	2 million people	Unauthorized access to a network server	Names, birth dates, addresses, provider, diagnosis and billing information, insurance numbers, medical record numbers, patient IDs	Zero-trust approach.
Broward Health Data Breach	Jan. 2022	1.3 million patients	Breach through a compromised third-party medical provider	Names, addresses, birth dates, driver's license numbers, insurance, and medical information	Enforce multi-factor authentication for accessing all endpoints, ensure secure privileged access management, and monitor all connections to endpoints diligently.
Morley Companies Data Breach	Feb. 2022	521,046 individuals	Ransomware attack	Names, addresses, SSN, birth dates, client ID numbers, medical diagnosis and treatment information, and health	The delay in notification heightened the risk of breaching the HIPSS Breach Notification rule; notifications should be made

				insurance information	promptly and directly.
L'Assurance Maladie Data Breach	Mar.2022	510,000 people	Retrieving the passwords for 19 accounts belonging to pharmacists from the dark web	Names, surnames, dates of birth, SSN, GP details, and level of reimbursement	Deploy multi-factor authentication and implement a data leak detection solution.
ARcare Data Breach	Feb. 2022	345,000 people	Maintaining unauthorized access inside computer systems, exposing on the internet, and stealing sensitive data for ransom	Names, SSN, driver's license numbers, state identification numbers, dates of birth, financial account information, medical treatment information, prescription information, medical diagnosis information, condition information, and health insurance information	Evaluate data security practices and explore advanced risk mitigation strategies.
OneTouch-Point (OTP)	July 2022	2.6 million people	Locking and encrypting files	Names, addresses, birthdays, medical records, patient demographics, employment dates and ID numbers, service descriptions and dates, test results, and diagnosis codes	Annual review of security policies.

5. Discussion:

Medical data generated and analyzed in modern healthcare vary a lot, such as electronic health records (EHRs), medical images, and patient monitoring data.

According to data collected for the period 2009 to 2023 (Wong) (Jeff Tully), 5,887 healthcare data breaches were reported for more than 500 records. These breaches showed that 519,935,970 healthcare records were disclosed. In the year 2018, 500 healthcare records were reported as disclosed, with the rate of record per day.

It shows that 30% of the cyber incidents that focused on data abuse targeted healthcare organizations, which means that healthcare centers and institutes are very desirable targets for cyber-attacks (Ramo SENDELJ).

Healthcare institutions invest billions of dollars ($65 billion) in cyber protection (Kinross), but they still facing a huge number of cyber-attacks. This number even continues increasing as many people do not report cyber incidents, which concludes that the number of cyber-attacks is significantly higher than the number that is reported.

As cybersecurity safeguards and technologies advance, so do the cleverness of attacks. It is essential to assume that a breach may have already occurred, prompting healthcare organizations to be prepared with comprehensive plans, recovery strategies, and countermeasures. The spread of mobile phones and other portable devices has introduced new opportunities for both healthcare providers and hackers. Employing well-established cybersecurity technology recommended by specialists is becoming more crucial. Validated measures and products should be utilized to mitigate the risks of breaches, bugs, and malfunctions. Cybersecurity approaches should function as a security filter, prioritizing effectiveness over inconvenience and reliability. By aligning cybersecurity and patient safety programs, businesses can safeguard patient safety and privacy while ensuring the continuity of effective, high-quality care delivery by minimizing disruptions that could compromise clinical outcomes.

Insiders, whether acting voluntarily or under pressure, commit cyber-attacks against their organizations. In both scenarios, insiders possess the necessary credentials to execute healthcare data breaches or other cybersecurity risks. An insider threat may involve a dissatisfied employee who illegally obtains Protected Health Information (PHI) from their employer's network and publishes it online to hit back against their former employer, whether acting independently, or with other criminals·

While connected technologies offer numerous benefits, they also attract cyberattacks and data breaches. Although external breaches exceed internal abuses as the primary source of security risks, internal misuse is more frequent in the healthcare sector than in other industries. Medical IoT (IoMT) devices are attractive targets for cybercriminals seeking valuable protected health information. To safeguard patients and their data, manufacturers must prioritize security in device design·

Various security techniques, all of which are cost-worthwhile, should be considered by medical institutions. Implementing multi-factor authentication can provide an additional layer of security for sensitive data and external access. Protected health information, among the most sensitive data on the internet, has seen increased volume and complexity as healthcare digitization advances. With each enhancement in automation and data analytics, the potential for compromise rises, necessitating a balanced approach to data protection and cybersecurity in healthcare.

Organizations allowing mobile logins may occasionally neglect to require secure equipment, leaving their networks vulnerable to malware and attackers due to ineffective planning or security measures concerning staff communication devices. Disposal of equipment during upgrades may expand the problem, as network information or passwords can remain accessible.

Medical equipment websites are attractive targets for hackers due to their often-careless security measures. Although infusion pumps primarily relay data to the attending physician and patient, they are constructed to interact with external platforms and transmit data as the Internet of Medical Things (IoMT) progresses. Unauthorized interception or manipulation of this data can result in various complications, granting hackers access to a broad array of network-connected devices, including equipment functionalities.

Data breaches affecting thousands of healthcare patients occur weekly, often due to human error such as falling for phishing scams. Given the healthcare industry's confidence in personnel for patient care, the risk of data breaches or security incidents is increased, underscoring the need for a robust information security management program. Hospitals, doctor's offices, and clinics have all been targeted by cybersecurity risks with significant consequences. Once a medical organization's system is breached, often due to an employee clicking on a suspicious email link, all patient files may be held hostage. Computer viruses can be transmitted via email, text messages, and websites, targeting unsuspecting and inexperienced end-users.

Conclusion

Within the domain of healthcare-related cyber insurance claims, unauthorized access emerges as the primary concern, followed by compromised data as the second most significant threat, and ransomware incidents thereafter. Most of the threats are outlined as follows:

- Unintentional data breaches.
- Malicious data breaches.
- Ransomware incidents.
- Lost or stolen devices.

Even with tough security procedures in place, healthcare information remains vulnerable due to the increasing strength of threats. Therefore, implementing additional cybersecurity measures is imperative to effectively address and prevent attacks on healthcare data.

References

Aaron Turransky, M. H. (2022). Artificial Intelligence and Cybersecurity: Tale of Healthcare Applications. In M. S.-k. M. Hadi Amini, *Cyberphysical Smart Cities Infrastructures: Optimal Operation and Intelligent Decision Making* (pp. 1-11).

Ekaterina Balandina, S. B. (2015). Iot use cases in healthcare and tourism. *Business Informatics (CBI)*, 37-44.

Irei, S. S. (n.d.). *What is ransomware? How it works and how to remove it*. Retrieved February 2024, from https://www.techtarget.com/searchsecurity/definition/ransomware#:~:text=Ransomware%20is%20a%20type%20of,accessing%20their%20files%20and%20systems.

Jeff Tully, J. S. (2020). Healthcare Challenges in the Era of Cybersecurity. *Health Security, 18*(3), 281-231. doi:10.1089/hs.2019.0123

Kim, L. (2017). Cybersecurity awareness: protecting data and patients. *Nursing Informatics*, 16-19.

Kinross, G. M. (2017). Cybersecurity and healthcare: how safe are we? *British Medical Journal*.

Kot, E. (2024, January 18). *14 Biggest Healthcare Data Breaches*. Retrieved from https://www.upguard.com/blog/biggest-data-breaches-in-healthcare

Ramo SENDELJ, a. I. (2022). Cybersecurity Challenges in Healthcare. *Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License 4.0 (CC BY-NC 4.0).*, 190-202.

Services, D. o. (2023). *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients.* USA.

Steven Furnell, M. P. (2001). Security Vulnerabilities and System Intrusions. *Network Research Group, Department of Communication and Electronic Engineering, University of Plymouth*, 87-96. doi:10.1007/0-306-47007-1_7

Suman, M. J. (2021). Dentistry 4.0 technologies applications for dentistry during COVID-19 pandemic. *Sustainable Operations and Computers*, 87-96.

US health insurer Anthem hit by massive data breach. (2015). *Computer Fraud & Security*, 1-3. Retrieved from www.healthcareinfosecurity.com/anthem-hit-by-massive-data-breach-a-7876

Wong, A. J. (2014). Healthcare Cybersecurity Risk Management: Keys To an Effective Plan, Biomed. *Instrument Technology*, 26-30.