European Economic Letters
ISSN 2323-5233
Vol 14, Issue 2 (2024)
http://eelet.org.uk

Strengthening Customer Data Protection in Healthcare: An Empirical Analysis of Data Privacy and Security Measures for Ensuring Customer Information Security

Prof. Vempali Visweswara Rao[1], Prathap Kumar. TA[2], Dr. M R. Jhansi Rani[3], Dr. Sheetal Mahendher[4], Prof. Leonard L[5], Dr. Naveen Pol[6]

1. Associate Professor, ISBR Business School
2. Student, ISBR Business School
3. Dr. M R. Jhansi Rani, ISBR Business School ISBR
4. Professor and Research Chair, ISBR Business School
5. Assistant Professor, ISBR Business School
6. Associate Professor, ISBR Business School ISBR

Abstract

In the healthcare industry, the security and privacy of consumer data are crucial. This empirical study explores into the critical issue of ineffective data privacy and security protections in the healthcare sector, exposing sensitive patient information to breaches and unauthorised access. The study intends to improve data protection procedures in order to preserve customer information, retain patient confidence, assure regulatory compliance, and ensure the continuity of high-quality healthcare services. By examining existing data privacy safeguards, technical improvements, and legislative frameworks, the report identifies the core causes of data vulnerabilities and makes practical solutions. The research is guided by three primary objectives: analysing the influence of data privacy and security measures on patient trust and confidence, measuring patient acceptance of Electronic Health Records (EHR), and investigating the link between data breach awareness and customer data privacy. In an era of increasing cyber threats and regulatory requirements, this study adds to the urgent need for stronger data protection in healthcare by emphasising the importance of maintaining patient trust and ensuring the integrity of medical systems in an interconnected digital environment.

Keywords: Healthcare, Data privacy, Data security, Customer information, Patient trust, Electronic Health Records (EHR)

Chapter 1: Introduction

1.1 Introduction to Data Digitalization

“Data digitalization has emerged as a transformative phenomenon across industries, revolutionizing the way information is managed, processed, and communicated. This process involves converting analogy data into digital formats, enabling its storage, analysis, and transmission through electronic devices and systems. The healthcare sector, in particular, has experienced a profound impact from data digitalization, reshaping the delivery of patient care, medical record management, and healthcare administration.

1.2 Benefits of Data Digitalization

There are several benefits to adopting data digitalization, and these benefits have fuelled its acceptance across numerous sectors. These advantages are especially obvious in the healthcare industry. First, digital data improves accessibility and efficiency. It is possible to easily access and retrieve patient information, medical histories, and test results, improving well-informed decision-making and accelerating patient treatment. The switch from paper-based records to digital formats also results in significant storage space savings, which translate into lower costs and better organised healthcare facilities.

Enhanced Data Accuracy and Integrity:

Data accuracy is important, especially in fields like healthcare where accuracy is essential. Handwritten documents are prone to mistakes, which can cause confusion or misinterpretation. Data digitization encourages standardised entry techniques and electronic documentation, which reduces human error. This increased precision guarantees that medical records stay consistent and trustworthy, lowering the possibility of medical mistakes brought on by inaccurate or lacking information.

Remote Access and Collaboration:

Data has become digital, transcending physical boundaries and allowing for remote access and cooperation. This is especially advantageous for telemedicine and remote consultations in the healthcare industry. Regardless of distance, medical practitioners may safely view patient information and communicate about situations with associates. This degree of accessibility improves the coordination of care across experts, resulting in a more thorough and all-encompassing approach to patient care.

Data Analytics and Insights:

Advanced data analytics may now be used thanks to the transfer of data into digital representations. To gain useful insights, organisations can evaluate patterns, trends, and correlations in data. Through the use of evidence-based decision-making, this competence can enhance patient outcomes in the healthcare industry. Data analytics may be used to better understand illness trends, develop effective treatments, and run healthcare facilities more effectively.

Improved Patient Care and Experience:

The treatment of patients may be directly impacted by data digitization in healthcare the most. Quick access to thorough patient histories by medical experts enables more individualised and successful therapy. Medical professionals may monitor changes in patient conditions over time using digital data, which helps in tracking the progression of chronic diseases or recovery. In the end, this leads to improved patient outcomes and experiences.

1.3 Challenges and Considerations in Data Digitalization:

“While data digitization has many advantages, it also presents a number of problems and issues that businesses must deal with in order to make the transition smoothly and continue to be successful. These difficulties cross organisational, technical, and ethical fronts, necessitating strategic planning.

Data Security and Privacy Concerns:

The increased danger to data security and patient privacy is one of the biggest obstacles to data digitization. Sensitive medical records and personal data are being digitised, which increases the attack surface for possible cyberattacks. To protect against data breaches, unauthorised access, and cyberattacks, healthcare organisations must make considerable investments in effective cybersecurity solutions. To guarantee patient trust and prevent legal penalties, compliance with data privacy laws such as GDPR in the European Union or HIPAA in the United States is essential.

Interoperability and Data Standardization:

Ensuring smooth data interoperability becomes more difficult when healthcare institutions deploy different electronic health record (EHR) systems. The interchange of patient data between organisations may be hampered by various systems' usage of dissimilar data formats or protocols. This lack of standardisation can lead to disjointed patient records, which can hinder coordinated treatment and increase the risk of medical mistakes. For seamless data exchange and care continuity across systems, healthcare stakeholders must collaborate to create data standards.

Data Quality and Integrity:

Errors in digital data are possible, whether they result from technical failures or human input. To guarantee that digital records correctly reflect patients' medical histories and situations, maintaining data quality and integrity is crucial. The identification and correction of anomalies that might jeopardise patient care and decision-making need routine audits, data validation procedures, and quality control methods.

Chapter 2: Research design

2.1 Statement of the Problem

“The security and privacy of customer data are of the utmost importance in the rapidly digitalized world of healthcare, where sensitive patient information is kept and transferred electronically. The healthcare sector confronts rising vulnerability to data breaches, unauthorised access, and cyber threats even as it welcomes technology improvements to improve patient care and operational efficiency. The most important topic to investigate is how to successfully strengthen data privacy and security measures to protect customer information in the healthcare domain, maintaining patient confidence, regulatory compliance, and the continuity of high-quality healthcare services. This study aims to identify the root causes of data vulnerabilities, identify best practises, and propose actionable recommendations to strengthen data privacy and security, strengthening the basis of client trust in healthcare services. It does this through an empirical analysis of current data protection measures, technological advancements, and regulatory frameworks”.

2.2 Need for the study

“This study has significance in an era of growing cyberthreats, regulatory requirements, and the critical importance of patient trust. The healthcare industry's susceptibility to data breaches puts patient privacy, regulatory compliance, and overall operational integrity at danger. The need for haste is clear as new complexity are brought about by data-driven healthcare and emerging technology. This research tackles the urgent need for strengthened data protection by empirically analysing current data privacy measures and offering creative remedies. In an interconnected digital environment, maintaining patient trust, guaranteeing regulatory compliance, and protecting the smooth provision of high-quality healthcare services all depend on strengthening customer data security”.

2.3 Objectives of the study

I. To analyse the impact of data privacy and security measures on patient trust and confidence

II. To assess patient perseverance towards Electronic Health Recodes (EHR)

III. To explore relations between Awareness of data breaches and Customer data privacy

2.4 Literature Review

Within the healthcare landscape, the escalating digitalization of patient records, coupled with mounting cyber threats, underscores the pressing importance of safeguarding sensitive customer information, Information Technology (IT)-related challenges such as inadequate integration of healthcare systems and poor healthcare information management are seriously hampering efforts to transform IT value to business value in the U.S. healthcare sector (Bodenheimer, 2005; Grantmakers In Health, 2012; Herrick, Gorman, & Goodman, 2010; The Kaiser Family Foundation, 2012). One promising breakthrough is the application of big data analytics. Data analytics that is evolved from business intelligence and decision support systems enable healthcare organizations to analyse an immense volume, variety and velocity of data across a wide range of healthcare networks to support evidence-based decision making and action taking (Watson, 2014; Raghupathi, 2014) , However, ’the more functions are performed across interconnected systems and devices, the more opportunities for weaknesses in those systems to arise, and the higher the risk of system failures or malicious attacks’ (Michels and Walden, 2018). However, research indicates consumers’ willingness to prioritise and pay more for higher security when they buy connected products, provided the security level is communicated in a comprehensible way, such as a security label (Johnson et al., 2020; European Com- mission, 2020a, 2020b). Furthermore, security vulnerabilities in robots raise significant concerns for manufacturers, programmers, and for those who interact with them in domains of sensitive applications such as healthcare. In a healthcare setting, robots interact in close, direct contact with children, older adults, and per- sons with disabilities and it may be unclear for the target user whether the robot is functioning properly or is under attack (Fosch-Villaronga et al., 2018). Cyber-physical systems may present a risk in case of cyberattacks. In 2015, a Jeep Cherokee was switched off remotely by hackers while being driven by a journalist.2 In another ex- ample, the Stuxnet virus subtly changed the speeds that the Iranian nuclear centrifuges spun, damaging or destroying the carefully calibrated machines (Holloway, 2015). These are examples that highlight the very real risks of exploiting the vulnerabilities of cyber-physical systems in general. These cybersecurity risks are also relevant for the context of service robots, because systems that exert direct control over the world can cause harm in a way that humans can- not necessarily correct or oversee (Amodei et al., 2016). Service robots interact with humans and, in the healthcare sector, users are often in a vulnerable position, which makes these risks more critical. For example, a teleoperated surgical robot has been hacked by researchers, and bodily harm might have been the consequence, if this had been done by a malicious hacker. The European Parliament also highlighted that ‘possible applications of AI and robotics in medical care (are) managing medical records and data, performing repetitive jobs (analysing tests, X-rays, CT scans, data entry), treatment design, digital consultation (such as medical consultation based on personal medical history and common medical knowledge), virtual nurses, medication management, drug creation, precision medicine (as genetics and genomics look for mutations and links to disease from the information in DNA), health monitoring and healthcare system analysis, among other applications’ (European Parliament, 2019). These applications are mainly software-based Artificial Intelligent (AI)-driven technologies, that may be embodied or not. On the other hand, the European medical device industry (COCIR, 2019) argues that there is a risk that “a patchwork of regulatory requirements may appear,” as Member States can introduce their requirements for cybersecurity certification, in addition to EU requirements. This statement highlights the challenges of integrating the two regulatory frameworks for physical safety and cybersecurity. Indeed, based on the rationale of the lex specialist principle, the more specific framework for medical devices might be used as an argument against mandatory cyber- security certificates for medical devices. Nevertheless, the requirements in the MDR are so general and abstract that there is a need for a more detailed framework for assessing cybersecurity requirements. Such a framework could be created either under the MDR or under the Cybersecurity Act (European Cybersecurity Act 2021).

2.5 Research Methodology

“The research methodology forms the backbone of this study, outlining the systematic approach and tools employed to achieve the research objectives effectively. This section delineates the strategies and techniques used to collect, analyse, and interpret the data necessary for comprehensively addressing the research questions. The qualitative aspect involves in-depth interviews with healthcare professionals to gain insights into their perspectives on data security practices and their perceived impact on patient trust. Quantitative data will be collected through structured surveys administered to a diverse sample of patients from various healthcare settings. These surveys will capture patient perceptions of data privacy and security measures and their resultant trust levels. Additionally, qualitative data will be gathered through semi-structured interviews with healthcare professionals responsible for data security implementations. Quantitative data will undergo statistical analysis, including correlation coefficients and regression modelling, to ascertain relationships between data security measures and patient trust. Potential limitations include self-reporting bias in surveys and the possibility of incomplete representation of data security practices due to variations across healthcare settings. This research methodology is designed to provide a comprehensive understanding of the intricate relationship between data privacy and security measures and patient trust in the healthcare sector. The mixed-methods approach ensures a holistic exploration, offering insights from both patients and healthcare professionals. The findings will aid healthcare institutions in making informed decisions to enhance their data security frameworks, ultimately fostering patient trust and ensuring the integrity of healthcare services in an increasingly digitized environment”.

Chapter 3: Framework of analysis

In this chapter, we will analyse the response that was gathered from 168 respondents using Google forms, including their reactions and opinions on ad-blocking software and the amazon digital marketing advertisements that were displayed across various online platforms. Using this information, I performed the following analysis.

3.1 Chi-Square Test

The “chi-square test” involves calculating the “chi-square test” statistic and comparing it with a chi-square distribution table that has a specific degree of freedom (df). The “degree of freedom” is determined by the number of categories in the contingency table. Once the test statistic is calculated, the “p-value” is computed. “The p-value reflects the probability of obtaining a test statistic as extreme or more extreme than the one observed". "A p-value of less than 0.05 indicates statistical significance, which means that the observed frequencies are unlikely to have occurred by chance".

The two categorical variable that we consider is one is Age group and another is Frequency of visiting hospital

Count of In the past 6 months, how many times have you visited a healthcare facility ?

Row Labels	18-25	25-30	30-40	35-40	Above 40	Grand Total
3-4 times	7	4	3	2	2	18
I did not visit	4	8	9	11	28	60
Multiple times	3	1	1	3	0	8
Once	10	6	4	11	17	48
Twice	13	3	4	5	9	34
Grand Total	37	22	21	32	56	168

Chi-square	**0.028254**

Hypothesis

H0 = "There is no significant association between the age and the frequency of visiting the hospital"

H1 = "There is a significant association between the age and the frequency of visiting the hospital"

Interpretation:

The corresponding "p-value" of the test statistic is p = 0.028254

Because the crosstabulation is a 2x4 table, the "degrees of freedom" (df) for the test statistic is 16

"Since the p-value is less than our chosen significance level (α = 0.05), we do reject the null hypothesis. Rather, we conclude that there is enough evidence to suggest an association between age and the frequency of visiting the hospital" .

Based on the results, we can state the following: "There is a significant association between the age and the frequency of visiting the hospital"

3.2 One-Way ANOVA

One-way ANOVA is a statistical test used to determine if there is a significant difference in the means of a continuous dependent variable between two or more independent groups. It assumes that the dependent variable is normally distributed and the variances are equal across groups. It is used to compare the means of a dependent variable across different levels or categories of a single independent variable. The independent variable is often categorical (e.g. type of treatment, type of group, etc.) and the dependent variable is continuous (e.g. height, weight, test scores, etc.).The results of a one-way ANOVA test can be used to determine if there is a significant effect of the independent variable on the dependent variable and to identify which specific groups are responsible for the significant effect.

Here we consider the education background and Accessing the health data in online

Anova: Single Factor						
SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		

Educational Background	168	366	3.26785714	0.63030888		
Accessing the health data in online	168	420	3.75	1.64864865		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	13.0178571	1	13.0178571	11.4243964	0.00085623	3.88368764
Within Groups	252.964286	335	1.13947876			
Total	265.982143	336				

Interpretation:

A p-value of 0.00085623 obtained from the ANOVA analysis involving educational background and accessing health data online suggests a statistically significant finding. This p-value indicates that there are substantial differences in the means of the dependent variable (such as perceptions, attitudes, or trust levels) across the various groups categorized by their educational backgrounds and their preference for accessing health data online. With a p-value significantly smaller than the conventional threshold of 0.05, there is strong evidence to reject the null hypothesis. This implies that at least one group among those defined by educational background and online health data access is significantly different from the others in terms of the dependent variable under consideration.

Hypothesis 1

H_0 = "There is no mean difference between the education background and Accessing the Electronic Health Recodes"

H_1 = "There is mean difference between the education background and Accessing the Electronic Health Recodes"

Observation and Results

- The statistical significance of the ANOVA model that was run is ($p < 0.05$), which is less than 0.05, and indicates that, overall, the ANOVA model statistically significantly to analyse the mean difference

- The "p-vale" is 0.00085623 which is less than the 0.05 so it will accept the alternative hypothesis H1

Result : **"**There is mean difference between the education background and Accessing the Electronic Health Recodes"

3.3 Regression analysis

Regression analysis is a statistical method used to examine the relationship between a dependent variable and one or more independent variables. It is a widely used tool in management research to understand how changes in independent variables affect changes in the dependent variable.

SUMMARY OUTPUT						
Regression Statistics						
Multiple R	0.99412611					
R Square	0.98828672					
Adjusted R Square	0.9880718					
Standard Error	1.30426657					
Observations	168					
ANOVA						
	df	*SS*	*MS*	*F*	*Significance F*	
Regression	1	15644.5699	7822.28497	4598.33817	5.533E-106	
Residual	166	185.42113	1.70111129			

Total	167	15829.9911				
	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*
Intercept	-5.9738469	0.73608559	-8.115696	7.9525E-13	-7.4327446	-4.5149492
Awareness of data breaches	0.87771738	0.02223096	39.4817545	2.135E-66	0.83365634	0.92177843

Lower 95.0%	*Upper 95.0%*
-7.4327446	-4.5149492
0.83365634	0.92177843

Interpretation:

From the above regression analysis we have found the relationship between the Awareness of data breaches and Customer data privacy from that we will find the hypothesis for the obtained tables . The multiple R value of 0.9941 suggests an extremely strong positive linear relationship between the independent variable (Customer data privacy) and the dependent variable (Awareness of data breaches). This high multiple R value indicates that variations in the independent variable are closely associated with variations in the dependent variable. In other words, as customer data privacy increases, awareness of data breaches also tends to increase proportionally. The p-value of 2.135E-66 is exceedingly small, significantly below the commonly used significance level of 0.05. This p-value indicates a highly statistically significant relationship between Customer data privacy and Awareness of data breaches. This means that the observed relationship between these two variables is unlikely to have occurred by chance.

Taken together, the multiple R value of 0.9941 and the extremely low p-value of 2.135E-66 suggest that Customer data privacy has a substantial and significant impact on the level of Awareness of data breaches. This finding implies that when customer data privacy measures are enhanced, there is a strong likelihood that awareness of data breaches among individuals will also increase. These results emphasize the importance of prioritizing robust data privacy practices to enhance awareness and vigilance regarding potential data breaches among customers.

Hypothesis 1

H_0 = “There is no significant relationship between the Awareness of data breaches and Customer data privacy”

H_1 = “There is a significant relationship between the Awareness of data breaches and Customer data privacy”

Observation and Results

The “*R* value” represents the simple correlation and is 0.9941which indicates a “high degree of correlation”

The statistical significance of the regression model that was run is ($p < 0.05$), which is less than 0.05, and indicates that, overall, the regression model statistically significantly predicts the outcome variable

The “p-vale” for the Construct 1 (Ad-acceptance & interest) is **2.135E-66** which is less than the 0.05 so it will accept the alternative hypothesis H1

Result : “There is a significant relationship between the Awareness of data breaches and Customer data privacy”

Chapter 4: Conclusions

4.1 Findings

“The research findings provide a comprehensive understanding of the complex relationships among data privacy measures, patient trust, awareness of data breaches, and the broader implications for healthcare information security.

Impact of Data Privacy and Security Measures on Patient Trust: In alignment with the research findings underscore the significant impact of data privacy and security measures on patient trust and confidence. This statistical significance indicates that different educational backgrounds and online data access preferences lead to variations in patient awareness and trust. These results emphasize the need for tailored communication strategies that address patients' diverse needs and preferences, fostering greater trust in healthcare data handling practices. Patient Perceptions of Data Security and its Trust Implications: The results pertaining to extracted from regression analysis, provide a deeper understanding of the intricate relationship between Customer data privacy and Awareness of data breaches. This demonstrates that as patients perceive heightened data privacy measures, their awareness of potential data breaches amplifies. Ultimately, this leads to increased trust, as patients recognize the importance of transparent and secure data handling practices. These findings accentuate the need for healthcare providers to actively engage patients in understanding data security protocols, fostering an environment of trust and empowerment. Exploring Relations between Awareness of Data Breaches and Customer Data Privacy: is illuminated through the regression analysis findings as well. The associated p-value further confirms the highly significant nature of this relationship. In essence, the research findings not only validate the study's objectives but also provide a nuanced understanding of the multi-dimensional aspects of data privacy, trust, and awareness within the healthcare domain. By harnessing the power of these findings, the healthcare industry can foster a culture of data protection, trust, and empowerment that ultimately benefits both patients and providers in an increasingly digital healthcare landscape”.

4.2 Conclusions

“The culmination of this research brings to light a cohesive understanding of the intricate interplay between data privacy, patient trust, awareness of data breaches, and their collective impact on the healthcare sector. The insights gleaned from the comprehensive analysis provide valuable implications for healthcare institutions, policymakers, and stakeholders as they navigate the evolving landscape of data security and patient confidence. Implications for Healthcare Trust and Security: The research findings underscore the pivotal role that data privacy measures play in shaping patient trust and awareness within the healthcare domain. The significant relationship identified between data privacy and patient trust reinforces the imperative for healthcare providers to cultivate an environment where transparent data security practices are upheld. As patients become increasingly aware of the measures in place to protect their information, their trust in healthcare institutions is fortified. This has significant implications for fostering patient engagement, satisfaction, and long-term loyalty. Transparency as a Pillar of Trust: The insights garnered from the examination of patient perceptions elucidate the importance of transparent communication in building and sustaining patient trust. The correlation between heightened data privacy perceptions and increased awareness of potential data breaches highlights the need for clear, accessible, and patient-cantered communication strategies. Healthcare organizations should seize the opportunity to communicate their commitment to data security, thus empowering patients to actively engage in safeguarding their information. Future Directions and Collaborative Initiatives: In light of the research outcomes, the path forward involves collaborative efforts between healthcare providers, regulators, and technology experts. Strengthening data privacy measures, promoting transparency, and offering patient-cantered educational initiatives stand as key strategies for building and maintaining patient trust. Furthermore, the study underscores the need for ongoing research to adapt to the evolving digital landscape and the emergence of new security challenges. In closing, this research has shed light on the intricate nexus of data privacy, patient trust, awareness of data breaches, and their far-reaching implications for the healthcare sector. By embracing these insights and forging collaborative paths, the healthcare industry can lay the groundwork for a secure, transparent, and patient-cantered digital healthcare era”.

Reference

1. Wang, Yichuan, et al. “Beyond a Technical Perspective: Understanding Big Data Capabilities in Health Care.” *IEEE Xplore*, 1 Jan. 2015, ieeexplore.ieee.org/abstract/document/7070183/.
2. “Big Data Analytics: Understanding Its Capabilities and Potential Benefits for Healthcare Organizations.” *Technological Forecasting and Social Change*, vol. 126, no. 1, Jan. 2018, pp. 3–13, https://doi.org/10.1016/j.techfore.2015.12.019.

3. Kaur, Prableen, et al. “Big Data and Machine Learning Based Secure Healthcare Framework.” *Procedia Computer Science*, vol. 132, 2018, pp. 1049–1059, www.sciencedirect.com/science/article/pii/S187705091830752X, https://doi.org/10.1016/j.procs.2018.05.020.
4. Sarkar, Bikash Kanti. “Big Data for Secure Healthcare System: A Conceptual Design.” *Complex & Intelligent Systems*, vol. 3, no. 2, 21 Mar. 2017, pp. 133–151, https://doi.org/10.1007/s40747-017-0040-1.
5. Dash, Sabyasachi, et al. “Big Data in Healthcare: Management, Analysis and Future Prospects.” *Journal of Big Data*, vol. 6, no. 1, 19 June 2019, pp. 1–25, journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0217-0, https://doi.org/10.1186/s40537-019-0217-0.
6. Hossain, M. Shamim, and Ghulam Muhammad. “Cloud-Assisted Industrial Internet of Things (IIoT) – Enabled Framework for Health Monitoring.” *Computer Networks*, vol. 101, June 2016, pp. 192–202, https://doi.org/10.1016/j.comnet.2016.01.009.
7. Fosch-Villaronga, Eduard, and Tobias Mahler. “Cybersecurity, Safety and Robots: Strengthening the Link between Cybersecurity and Safety in the Context of Care Robots.” *Computer Law & Security Review*, vol. 41, July 2021, p. 105528, https://doi.org/10.1016/j.clsr.2021.105528.
8. Randeree, Ebrahim, and H.R. Rao. “E-Health and Assurance: Curing Hospital Websites.” *International Journal of Electronic Healthcare*, vol. 1, no. 1, 2004, p. 33, https://doi.org/10.1504/ijeh.2004.004653. Accessed 27 Oct. 2019.
9. Semantha, Farida Habib, et al. “A Systematic Literature Review on Privacy by Design in the Healthcare Sector.” *Electronics*, vol. 9, no. 3, 7 Mar. 2020, p. 452, www.mdpi.com/2079-9292/9/3/452/htm, https://doi.org/10.3390/electronics9030452.
10. Palanisamy, Venketesh, and Ramkumar Thirunavukarasu. “Implications of Big Data Analytics in Developing Healthcare Frameworks – a Review.” *Journal of King Saud University - Computer and Information Sciences*, vol. 31, no. 4, 1 Oct. 2019, pp. 415–425,www.sciencedirect.com/science/article/pii/S1319157817302938, https://doi.org/10.1016/j.jksuci.2017.12.007.