CONFERENCE ARTICLE

A STUDY ON CHALLENGES OF DATA SECURITY AND DATA PRIVACY IN THE HEALTHCARE SECTOR: SWOT ANALYSIS

Asha Prasuna, Avani Rachh*

K J Somaiya Institute of Management, Somaiya Vidyavihar University (SVU), Vidyavihar (E) Mumbai 400077, India

Correspondence: ashasivakumar@somaiya.edu

ABSTRACT

OBJECTIVE

The aim of this research paper is to analyse and provide suggestions to overcome challenges of data security and data privacy in the healthcare sector. The objective is to also conduct a SWOT analysis to understand the current scenario of the healthcare sector. It will provide detail on the concerns of the healthcare sector.

DESIGN AND SETTING

A quantitative data analysis was conducted. The online Google forms were used to gather primary data. Statistical analysis software was used for data analyses like independent sample t-tests and one-way anova.

RESULTS

The healthcare sector is concerned about data security and data privacy. The violation of privacy cases in India has increased over several years. The data security and data privacy in healthcare sector are very important. The female respondents felt that it is very important that their consent is taken before their personal information is sold or shared with others plus before tracking their movement on the internet than male respondents.

CONCLUSION

Healthcare and information technology sectors are among the most important sectors in the current online world. The strengths are healthcare awareness and mobile applications while weakness are ineffectively protected systems and infrastructure problems. The opportunities are investments for different facilities in the sector plus increase in research and development. The threats are violation of data privacy, data thefts and cyber-attacks putting a question on data security. Proper effective procedures have to be implemented to improve data security.

2nd International Healthcare Management Conference 2022 - Navigating the New Normal with Focus on Healthcare Accessibility, Innovation and Sustainability

KEYWORDS

data security, data privacy, SWOT analysis, challenges, healthcare sector.

INTRODUCTION

The healthcare sector has played an important role in the current pandemic. The sector has benefited from information technology by providing information about health care, medical facilities, COVID-19 vaccinations, etc. on different websites and mobile applications (usually known as "apps."). They are application software that run on mobile devices. The hospitals, pathology laboratories, diagnostic centres, pharmacy plus medical stores etc. use websites and mobile applications to connect with people.

People can online book medical tests, order medicines, procure medical reports, etc. on different websites and apps. India's Ministry of Health and Family Welfare has developed (https://www.cowin.gov.in/) an online facility for people to book online vaccination slots and get digital vaccination certificates which accomplish the task of vaccine passports [1]. All of these websites and apps collect a lot of personal and medical data of patients. A Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis of healthcare sector was conducted to understand the strength, weakness, opportunities and threats faced by this sector. As per our SWOT analysis, it is a challenging task to secure and protect all data. It is important to secure data. The Indian data security market was worth $USD99.55 million in 2019 and it has been forecasted to be $USD261 million by 2025 [2].

Data security methods are used by organisations to protect data from cyberattacks, data breaches and data losses. Data privacy is related to access of personal information by authorised people plus organisations and simultaneously the person retains control over it [3]. The main challenges of data security in healthcare sector are security of mobiles plus data stored in them, computers and medical devices, software updates, remotely scanning all devices for anti-viruses, phishing attacks and data breaches [4]. The main challenges of data privacy in healthcare sector are legislative gaps, absence of trust due to lack of privacy and patients don't have control over shared medical records [5].

A digital health passport survey was conducted in February 2021. Respondents were youth foreign travellers. The main worries were related to data security and data privacy. The first security worry was hacking of individuals' information. The second worry was concern about privacy when it comes to sharing of health information. The third worry was about the absence of transparency and control over shared data [6]. The number of cybercrime cases related to violation of privacy in India has increased from 62 in 2014 to 742 in 2020 but the conviction rate for violation of privacy is very low [7].

Overall, hardly any research was conducted to find out the views of the users about data security and data privacy. What is lacking today? The willing consents of website and app users are not requested/taken. It is users' personal data and they are under duress to provide the same, if they have to use different health related websites plus mobile applications including India's COVID-19 vaccine registrations. In many times the users' data are misused. An effort is made to understand their viewpoints on this and provide the suggestions to improve the situation.

SWOT ANALYSIS

Strengths of healthcare sector are economical treatments, availability of generic drugs, increasing healthcare awareness, willingness to pay for quality healthcare and mobile applications for different healthcare facilities. Big data will help organisations to analyse it. It helps the organisations to take effective decisions for business growth. The data can be accessed from any location, easy to use and maintain.

Weaknesses are infrastructure deficiency, inadequately protected systems, limited medical and information technology specialists. Some of the organisations do not have enough data storage facilities creating problems for data access as well as for data sharing among employees to complete a particular task. It could happen due to poor information system planning. The implementation of laws is poor. Some work environments are toxic. Inadequate training to users with respect to applications and systems. Poor mobile networks and internet facilities are also issues.

Opportunities are more awareness about healthcare, life expectancy has increased, medical tourism, more medical colleges, foreign direct investments in infrastructure plus research and development. Better healthcare facilities will increase lifestyle support and public health. It will also reduce cost and increase fraud detection. New business models will be developed and specific treatments can be provided. Low cost skilled and qualified employees are available in India. The launch of 5G network will improve the capacity plus coverage of mobile networks and internet speeds in India.

Threats are costly treatments in private plus super-speciality hospitals, import duties on medical equipments, human errors, counterfeit medicines, cyberattacks like ransomwares', data thefts and violation of data privacy. Many times government healthcare facilities are not maintained properly. Corruption is also a problem. The other concern is brain drain in medical field. The main issues are data privacy, securing data, unauthorised use of information plus selling data and information for pecuniary benefits. [8] [9] [10] [11] [12]

METHODS

RESEARCH OBJECTIVES

- To carry out a SWOT analysis of healthcare sector.
- To find out challenges of data security and data privacy in healthcare sector.
- To find out opinions of the respondents about importance of their consent regarding data privacy with respect to types of mobile plans.
- To find out number of cybercrime cases reported under violation of privacy in India.

RESEARCH METHODOLOGY

The SWOT Analysis was conducted to know the threats faced by the healthcare sector. This strategic analytical tool provided detail of the main challenges encountered by the healthcare sector. It became a base for collecting primary data to understand the concerns of health related websites and app users. The primary data were gathered for empirical research analysis. Quantitative research techniques were used for analysis. Online survey was conducted to collect primary data and tool used was Google Forms. The sample size of primary data was 192. The respondents were major internet users in the age group of 20 to 30 years from Mumbai, India.

DATA ANALYSIS

The data analyses were done using SPSS statistical analysis software. The data analyses like frequency distributions, independent sample t-tests and one-way anova were conducted.

HYPOTHESES

The Independent Sample T-Tests and One-Way Anova were conducted on primary data. The hypotheses statements for Independent Sample T-Tests were as follows:

- Ho1: There is no significant difference in opinions of the respondents about before installing applications, do they read application provider's privacy policy for using application with respect to gender.
- Ho2: There is no significant difference in opinions of the respondents about authentication systems used to lock mobile screens for security with respect to gender.
- Ho3: There is no significant difference in opinions of the respondents about content providers have the right to sell information about its users to other companies with respect to gender.
- Ho4: There is no significant difference in opinions of the respondents about importance of their consent regarding data privacy with respect to gender for all the attributes.

The One-Way Anova hypothesis statement was as follows: Ho5: There is no significant difference in opinions of the respondents about importance of their consent regarding data privacy with respect to types of mobile plans for all the attributes.

RESULTS

The questionnaire asked questions related to gender and for how many years respondents hve been using the internet. Respondents were also asked about the type of mobile plans used. The mobile plans are of two2 types: Pre-paid and Post-paid. In case of pre-paid mobile plans, the user pays the full amount in advance and gets the mobile service for a fixed number of days. While in case of post-paid plans, the user gets the bill after using the service for a month. The user generally gets two weeks to pay the monthly bill amount. Some of the respondents used both types of mobile plans. The respondents were also asked about whether they give importance to convenience or privacy?

The SWOT Analysis was the base for the following questions using Google Forms:

1. Before installing an application, do you read application provider's Privacy Policy for using applications?
2. What authentication system do you use to Lock Screen for security?
3. Whether content providers have the right to sell information about its users to other companies?

4. How important is their consent with respect different parameters related to data privacy?

Question numbers 1 had 3 options: never, sometimes and always. Question number 2 had 6 options: none, pin, password, pattern, fingerprint and face. Question number 3 had options based on a 5 points Agree Likert scale. Question number 4 had options based on a 5 points Important Likert scale. Question numbers 1, 3 and 4 required the respondents to select only one option while for question number 2 they had choice to select multiple options.

The sample size contains 95 males and 97 females. Seventy-five percentage of males and 78% of females use pre-paid mobile plans. Seventy-one percentage of pre-paid, 79% of post-paid and 73% of both mobile plan users gave importance to privacy over convenience. The questionnaire had third gender as an option but no one selected. Therefore, Independent Sample t-test was conducted on two groups i.e. male and female. The first three Independent Sample T-Tests null hypotheses were accepted as significance value was more than 0.05 at 95% confidence level.

The Independent Sample T-Tests null hypothesis i.e. Ho4: "There is no significant difference in opinions of the respondents about importance of their consent regarding data privacy with respect to gender for all the attributes" had six attributes. The three attributes of null Independent Sample T-Test hypothesis were accepted as the significance value was greater than 0.05 at 95% confidence level. The three attributes of the null Independent Sample T-Test hypothesis i.e. Ho4: "There is no significant difference in opinions of the respondents about importance of their consent regarding data privacy with respect to gender" were as follows:

- Sites track your movement around their site.
- Sites track your online purchases.
- Sites customize your online experience to your personal preferences.

The significance values of the other three attributes were less than 0.05. So, they were rejected at 0.05 significance level as p values are less than a. Therefore, the other three attributes for alternative hypothesis i.e. Ha4: "There is significant difference in opinions of the respondents about importance of their consent regarding data privacy with respect to gender" were accepted and the attributes were as follows:

- Sites sell/share your personal information with others.
- Sites track your movement around the Internet.
- Sites gather in-depth personal profiles about you from other outside databases.

To find out the difference between the three attributes the values in the Table 1 refer. The female group had a higher mean as compared to male group for all the three attributes and for rest of the attributes opinions of respondents were same for both male and female groups.

TABLE 1: PARTICIPANT GROUP STATISTICS FOR THIS STUDY

	Gender	N	Mean	Std. Deviation	Std. Error Mean
Sites sell/share your personal information with others	Male	95	4.52	0.944	0.097
	Female	97	4.76	0.658	0.067
Sites track your movement around the Internet	Male	95	4.41	0.905	0.093
	Female	97	4.73	0.654	0.066
Sites gather in-depth personal profiles about you from other outside databases	Male	95	4.35	1.070	0.110
	Female	97	4.68	0.798	0.081

The One-Way Anova was conducted as three types of mobile plans were considered while preparing the questionnaire. The three types of mobile plans are pre-paid, post-paid and both. According to Table 2, One-Way Anova null hypothesis i.e. Ho5 statement was accepted for all the attributes as significance (2-tailed) value was more than 0.05 at 95% Confidence Level.

TABLE 2: ANOVA TABLE – THREE TYPES OF MOBILE PLAN IN THIS STUDY

		Sum of Squares	df	Mean Square	F	Sig.
Sites sell/share your personal information with others	Between Groups	1.590	2	.795	1.187	.307
	Within Groups	126.613	189	.670		
	Total	128.203	191			
Sites track your movement around their site	Between Groups	.296	2	.148	.130	.878
	Within Groups	214.517	189	1.135		
	Total	214.813	191			
Sites track your movement around the Internet	Between Groups	.051	2	.026	.039	.961
	Within Groups	122.928	189	.650		
	Total	122.979	191			
Sites track your online purchases	Between Groups	.013	2	.007	.008	.992
	Within Groups	156.799	189	.830		
	Total	156.812	191			
Sites gather in-depth personal profiles about you from other outside databases	Between Groups	1.068	2	.534	.584	.559
	Within Groups	172.885	189	.915		
	Total	173.953	191			
Sites customize your online experience to your personal preferences	Between Groups	.092	2	.046	.040	.961
	Within Groups	219.903	189	1.164		
	Total	219.995	191			

DISCUSSION

The willing consent of the user with respect to collecting private data is not taken. The majority of the respondents gave priority to privacy in comparison to convenience. The findings match with other research work where the patient's consent is not taken for data sharing. The questions were raised whether patients will give consent for sharing their personal data as it invades data privacy and due to challenges of data security [13]. In the same way most of the respondents are not bothered to read application provider's privacy policy before installing applications as it is one sided. The users cannot use the applications, if they don't accept the privacy policies. The impression is that it is useless to read the same.

The other work also raised the consent of the user with respect to data sharing. It does not mean the consent to use or share the contact details of his or her family members and friends [14]. The Wall Street Journal had established that in 2011, 56% of the mobile applications collected the mobile's unique identification number plus 47% of the mobile applications gathered location of mobile devices and provided the information to third parties without the user's consent or awareness. Again in 2015, forty-seven percent of iOS and seventy-three percent of Android applications gathered private information like email addresses, location of mobile devices and passed on to third parties [15]. The situation has not changed from 2011 to 2023. The current research also points to the same findings. More research can be done on the importance of consent of application and website users. It is important as their private data are collected. It is the duty of the application and website developers to safeguard the data and not to invade the users' privacy.

LIMITATIONS

The primary data was collected in a short period therefore the sample size was only 192 respondents. The secondary data was downloaded from online sources due to pandemic, paucity of time and resources.

IMPLICATIONS

The survey was conducted to understand the opinions of respondents. The system is collecting their personal data but users are not aware about how it is used? The data collected by health related applications are shared with third parties. The users don't have control over their personal data. Most of the applications force the users to give access to their mobile devices cameras, microphones, phone, contacts, messaging services, location, photos and videos, music plus audio, notifications, nearby devices, etc. to use the applications and websites. The mobile applications cannot be used, if their accesses are denied by the users. Most of the time this type of access is ideally not required for using the application or website. However, the users are forced to agree to one-sided privacy policies of these applications invading data privacy. Many times hackers hack the servers and collect the private data including medical records of the patients. It is a data security issue.

The healthcare sector had cost wise the highest average breach worth $USD7.13 million in 2020 which had increased by 10.5% from 2019 [16]. The number of cybercrime cases like hacking, data breaches and violation of privacy has increased. The current Information Technology Act is inadequate to protect data privacy. Therefore, the Indian Data Protection Bill, 2021 is framed and expected to become an Act soon. It will protect personal plus non-personal data and data breaches have to be reported within 72 hours [17].

The application developers should not ask for any kind of access to devices like mobiles, laptops, etc. of the users. It will lessen the data privacy issue and burden on the organisations for securing systems and data. It will reduce the workload of the government agencies to solve cybercrime cases as the number of cases will come down.

CONCLUSION

The aim was to gather viewpoints of users with respect to different aspects of data security and data privacy. The purpose was to know whether the users' consent is taken with respect to collection of private data by health related mobile applications and websites.

Health related data is ever increasing. It is stored on different devices and that brings more challenges for securing the same. Hackers are targeting these devices to get medical records which can be used to blackmail and humiliate people. It is important to encrypt data, take data backups and have them at different locations, educate employees and conduct security audits [18]. The control of patients' personal data, transparency and data privacy are the main concerns as new medical applications are developed. Better data security and data privacy laws with standards and effective implementations of the same are the need of the hour in order to avoid cyber threats.

Data protection policies and strategies will help healthcare sector to secure data from external plus internal threats. It will also help the sector to obey the laws of the land with respect to data security and data privacy [19]. More resources and time are required to conduct research to understand the challenges faced worldwide and provide country specific solutions.

References

1. Co-WIN [Internet]. Cowin.gov.in. 2023 [cited 2023 Jan 22]. Available from: https://www.cowin.gov.in/
2. India: Data security market size 2025 | Statista [Internet]. Statista. Statista; 2019 [cited 2022 Jan 4]. Available from: https://www.statista.com/statistics/1197259/india-data-security-market-size/
3. Data Privacy vs. Data Security: What Is the Real Difference? [Internet]. Netwrix.com. 2019 [cited 2022 Jan 5]. Available from: https://blog.netwrix.com/2019/06/25/data-privacy-vs-data-security-what-is-the-real-difference/
4. 5 Data Security Challenges in Healthcare [Internet]. Health Administration Degrees. 2021 [cited 2022 Jan 3]. Available from: https://www.healthadministrationdegrees.com/articles/data-security-challenges-in-healthcare/
5. Top 3 issues facing patient privacy [Internet]. Healthcare IT News. 2012 [cited 2022 Jan 5]. Available from: https://www.healthcareitnews.com/news/top-3-issues-facing-patient-privacy
6. Rebuild Travel Digital Health Survey Reports | Amadeus [Internet]. Amadeus | The leading travel technology company. 2021 [cited 2022 Jan 5]. Available from: https://amadeus.com/en/insights/research-report/rebuild-travel-digital-health-survey-reports
7. Crime In India | National Crime Records Bureau [Internet]. Ncrb.gov.in. 2021 [cited 2022 Jan 4]. Available from: https://ncrb.gov.in/en/crime-india
8. Dias C, Santos M, Portela F. A SWOT Analysis of Big Data in Healthcare. Proceedings of the 6th International Conference on Information and Communication Technologies for Ageing Well and e-Health. 2020. Available from: https://www.scitepress.org/Papers/2020/93902/93902.pdf
9. Ganesan L, R.Senthamizh Veena. "Make In India" For Healthcare Sector in India: A SWOT Analysis on Current Status and Future Prospects [Internet]. ResearchGate. unknown; 2019 [cited 2022 Jan 4]. Available from: https://www.researchgate.net/publication/332292618

_'Make_In_India'_For_Healthcare_Sector_in_India_A_SWOT_Analysis_on_Current_Status_and_Future_Prospects

10. Pereira R, Salazar M, Abelha A, Machado J. SWOT Analysis of a Portuguese Electronic Health Record. IFIP Advances in Information and Communication Technology [Internet]. 2013 [cited 2022 Apr 17];169–77. Available from: https://ifip.hal.science/IFIP-AICT-399/hal-01470531
11. S. A, Dhastagir Sultan S. Health Care Delivery in India - SWOT Analyses. International Archives of Public Health and Community Medicine [Internet]. 2019 Aug 2 [cited 2022 Apr 17];3(2). Available from: https://clinmedjournals.org/articles/iaphcm/international-archives-of-public-health-and-community-medicine-iaphcm-3-024.php?jid=iaphcm
12. Indian healthcare to prioritize cyber security and put in place robust data privacy framework [Internet]. Pharmabiz.com. 2021 [cited 2022 Jan 3]. Available from: http://www.pharmabiz.com/NewsDetails.aspx?aid=143687&sid=1
13. Handler I. Data Sharing Defined—Really! Computer [Internet]. 2018 Feb 1 [cited 2022 Apr 16]; 51(2):36–42. Available from: https://search.ebscohost.com/login.aspx?direct=true&AuthType=cookie,ip,uid,url&db=edseee&AN=edseee.8301118&site=eds-live
14. Isaak J, Hanna MJ. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. Computer [Internet]. 2018 Aug [cited 2022 Apr 17];51(8):56–9. Available from: https://ieeexplore.ieee.org/abstract/document/8436400
15. Published by: Department of the Taoiseach on behalf of the Government Data Forum, January 28th 2016 Authored by: Rob Kitchin, NIRSA, Maynooth University Suggested citation: Kitchin, R. (2016) Getting smarter about smart cities: Improving data privacy and data security. Data Protection Unit, Department of the Taoiseach, Dublin, Ireland. Available from: https://www.researchgate.net/publication/293755608_Getting_smarter_about_smart_cities_Improving_data_privacy_and_data_security
16. 100 Data Privacy and Data Security statistics – Data Privacy Manager [Internet]. Data Privacy Manager. 2020 [cited 2022 Jan 2]. Available from: https://dataprivacymanager.net/100-data-privacy-and-data-security-statistics-for-2020/
17. Rao S. Parliament Annual Round-Up 2021 [Internet]. Livelaw.in. Live Law; 2021 [cited 2022 Jan 2]. Available from: https://www.livelaw.in/top-stories/parliament-annual-round-up-2021-188545
18. Trevor Morgan. The Data Security Challenges Faced by the Healthcare Industry - [Internet]. Thejournalofmhealth.com. 2021 [cited 2022 Jan 3]. Available from: https://thejournalofmhealth.com/the-data-security-challenges-faced-by-the-healthcare-industry/
19. DQINDIA Online. Data privacy and protection: A must for the healthcare sector [Internet]. DATAQUEST. 2021 [cited 2022 Apr 16]. Available from: https://www.dqindia.com/data-privacy-protection-must-healthcare-sector/