Asia-Pacific Journal of Health Management

RESEARCH ARTICLE

# A STUDY OF FUTURE OPPORTUNITIES AND CHALLENGES IN DIGITAL HEALTHCARE SECTOR: CYBER SECURITY VS. CRIMES IN DIGITAL HEALTHCARE SECTOR

*Avani Rachh*

Somaiya Institute, India

Correspondence: avanir@somaiya.edu

## ABSTRACT

### OBJECTIVE

The current study is to understand the opportunities for and challenges faced by digital healthcare sector. The aim of the study is to suggest measures for securing data and information collected by the sector plus have safer online transactions.

### DESIGN AND SETTING

The secondary data was collected from reliable sources. The primary data was collected online. The quantitative and qualitative analysis was done on data. The data was statistically analysed for this research article.

### RESULTS

Even though healthcare sector has spent on digital health and cybersecurity but still the number of cybercrime cases have increased. An attempt is made to understand the factors that can influence the number of cybercrime cases.

### CONCLUSION

The healthcare sector has opportunities in digital healthcare field in the current pandemic situation. At the same time, it has challenges to reduce the cybercrime cases as hackers are stealing confidential data and to take stringent measures to reduce the same.

### KEYWORDS

Healthcare Sector, Digital Healthcare Sector, Opportunities, Challenges

## INTRODUCTION

Healthcare sector has helped humankind in present covid pandemic situation. People are working from home but some sectors have opened up. People have to travel from their home to work and are prone to be infected. In some countries, the number of cases has increased and governments were forced to announce lockdown again. The health of citizens is more important. More people have started using digital healthcare facilities like mobile applications to contact doctors and order medicines online. Due to current pandemic scenario, digital healthcare sector has many opportunities and challenges like safeguarding online data.

Digital healthcare is an important part of healthcare system. It helps patients who are at home to connect with doctors. It reduces costs due to use of information, communication and technology. The medical records can be stored and accessed electronically known as Electronic Health Records (EHR). Mobile applications help to monitor health conditions. Digital healthcare has been used in the past also but now it has gained more importance than traditional healthcare systems, as it provides effective and ethical healthcare. [1]

Introduction of technology in everyday activities has provided many opportunities and challenges to data and information including infrastructure. [2] While in current and post Covid situations digital healthcare is most affected. The growth has increased multi-fold and will grow rapidly in the future. [3] Digital healthcare market is estimated to grow rapidly from USD $106 billion in 2019 to USD $640 billion in 2026. [4]

Healthcare sector has taken lot of burden in 2020 due to the Covid pandemic. It has given a boost to the digital healthcare sector and at the same time, new challenges are springing up. One of the main challenges is to safeguard data as we use digital platforms for health. [5] The other challenges are privacy, data breaches, data security, identity theft and cyber-attacks. [6]

The United States of America has dedicated acts for protecting health records and data privacy. Very few countries like United Kingdom, European Union, Australia, Canada, Singapore, Japan and New Zealand have specific rules, regulations, provisions or guidelines in their laws to safeguard personal information and data including electronic documents plus privacy. The authors have divided the health records in 3 groups based on sensitivity level. The first group is normal which can contain personal plus social data and identity theft can be the possible crime. The second group is called sensitive and includes financial information and has risk of frauds. The last cluster is named highly sensitive and comprises of data related to health risks plus clinical diagnoses. The possible crime for the third group could be extortion. Fifty-eight percentages of data breaches are done by insiders. With opportunities comes the threats like hacking, ransomware, phishing plus privilege abuse and challenges to Electronic Medical Records (EMR) infrastructure or system. [7]

The healthcare software developing companies have to take extra precautions to safeguard personal data collected by them. The issues elevated in such conditions are ethical, moral plus legal in nature. The companies have to follow confidential guidelines and deal with challenges like cyber privacy and security. [8]

### CYBER CRIME CASES RELATED TO HEALTHCARE SECTOR

In 2019, among the top five Indian cybercrime cases the major one was a hacking attacks on Indian healthcare website. The hacker stole 68 lakh records of doctors and patients. [9] In September 2020, Chinese hackers stole Spanish Research Centre's information related to Covid-19 vaccine. [10] In September 2020, German hospital and Universal Health Services (UHS) health system at 400 locations faced ransomware attacks. The five healthcare organisations reported that their data was stolen and available on the dark web by different hacker groups. [11] Many cybercrime cases are reported in India.

## METHODS

### RESEARCH OBJECTIVES

- To find out current situation of digital healthcare sector.
- To analyse global healthcare plus healthcare cybersecurity fundings and global cybersecurity market.
- To analyse corporate funding for digital health.
- To find out number of cybercrime cases reported in India.
- To find out cybercrime cases relating to healthcare sector.
- To analyse factors affecting security measures or precautions.

### RESEARCH METHODOLOGY

The quantitative and qualitative research analysis are done. Primary and secondary data are collected. Secondary data are collected from different sources. [12] [13] [14] The questionnaire method was used for primary data collection. The primary data was collected online using Google Form. The sample size of primary data is 111.

### DATA ANALYSIS

Microsoft Excel and statistical analysis software like PSPP, JASP (R based) are used for data analysis like frequency distribution, charts, correlation and factor analysis. [15] The

Descriptive Analysis like Mean, Standard Deviation and Percentages were also computed.

## HYPOTHESES

Independent Sample T-Test is used to analyse the primary data.

- $H_o$: To identify responses about willingness to provide information using mobile phone with respect to gender.
- $H_o$: To identify the responses about "There should be new laws to protect privacy on the Internet" with respect to gender.

Correlation is used to identify relationship between variables.

- $H_o$: The correlation between Annual Global Healthcare Funding and Annual Global Corporate Funding for Digital Health is not statistically significant.
- $H_o$: The correlation between Annual Global Healthcare Funding and Annual Global Healthcare CyberSecurity Funding is not statistically significant.
- $H_o$: The correlation between Annual Global Corporate Funding for Digital Health and Annual Global Healthcare CyberSecurity Funding is not statistically significant.
- $H_o$: The correlation between Annual Global Corporate Funding for Digital Health and Number of Cyber Crime Cases Reported in India is not statistically significant.
- $H_o$: The correlation between Annual Global Cybersecurity Market and Number of Cyber Crime Cases Reported in India is not statistically significant.

# RESULTS

The annual global healthcare funding has increased from $34,361 million from 2016 to $80,612 million in 2020, while number of annual global healthcare deals have increased from 4,140 to 5,523 from 2016 to 2020. Seventy-eight percentage of males felt privacy is more important than convenience, while 91% of females felt the same.

The Null Hypothesis, to identify responses about willingness to provide information using mobile phone with respect to gender was accepted as significance (2-tailed) value is more than 0.05 at 95% Confidence Level. The Null Hypothesis, to identify the responses about "There should be new laws to protect privacy on the Internet" with respect to gender was accepted as significance (2-tailed) value is more than 0.05 at 95% Confidence Level.

The strong positive correlation was found at 95% level for all the hypotheses statements. Therefore, we can say that there is correlation between all the mentioned variables. It means that even after spending on security, the number of cyber crime cases in India are increasing. It is necessary to overcome these challenges.

## FACTOR ANALYSIS

The Factor Analysis was done to understand the security measures or precautions taken by respondents to safeguard the data and information from cyber fraudsters, etc. The respondents were requested to provide their responses for the following statements relating to information security:

1) V1 = I respond to messages asking for urgent action due to security reasons.
2) V2 = I check padlock icon of the browser.
3) V3 = I click on links from any unknown person.
4) V4 = I share my financial or personal information by e-mail or text message.
5) V5 = I destroy the pin mailer after memorising the pin and/or change the pin after the first usage.
6) V6 = I keep my pin and ATM card /debit card /credit card together.
7) V7 = I disclose my internet banking password with anybody including my family members.
8) V8 = I respond to online offers that require me to provide my account details "for verification".
9) V9 = I always check the last log-in to my Internet Banking account.
10) V10 = I use the virtual keyboard/keypad to enter the user name/login and password for online banking.

### a) Preliminary Analysis

As per Table 1, determinant value is .253, which is more than .00001. Hence, multicollinearity is not a problem for these data. So, no need to eliminate any questions. The Pearson's Correlation Heatmap (Figure 1) shows correlation between the variables in graphical way.

### TABLE 1: PEARSON'S CORRELATION MATRIX

| VARIABLE | V1 | V2 | V3 | V4 | V5 | V6 | V7 | V8 | V9 | V10 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1. V1 | — | | | | | | | | | |
| 2. V2 | 0.16 | — | | | | | | | | |
| 3. V3 | 0.171 | 0.059 | — | | | | | | | |
| 4. V4 | 0.093 | -0.1 | 0.352*** | — | | | | | | |
| 5. V5 | 0.019 | 0.125 | -0.01 | 0.09 | — | | | | | |
| 6. V6 | 0.067 | 0.188* | 0.169 | 0.119 | 0.222* | — | | | | |
| 7. V7 | -0.001 | -0.083 | 0.29** | 0.341*** | 0.052 | 0.306** | — | | | |
| 8. V8 | 0.097 | -0.037 | 0.38*** | 0.252** | 0.008 | 0.322*** | 0.433*** | — | | |
| 9. V9 | 0.12 | 0.284** | 0.05 | -0.17 | 0.18 | 0.141 | 0.09 | 0.105 | — | |
| 10. V10 | 0.07 | 0.271** | 0.214* | -0.078 | 0.05 | 0.239* | 0.127 | 0.143 | 0.292** | — |

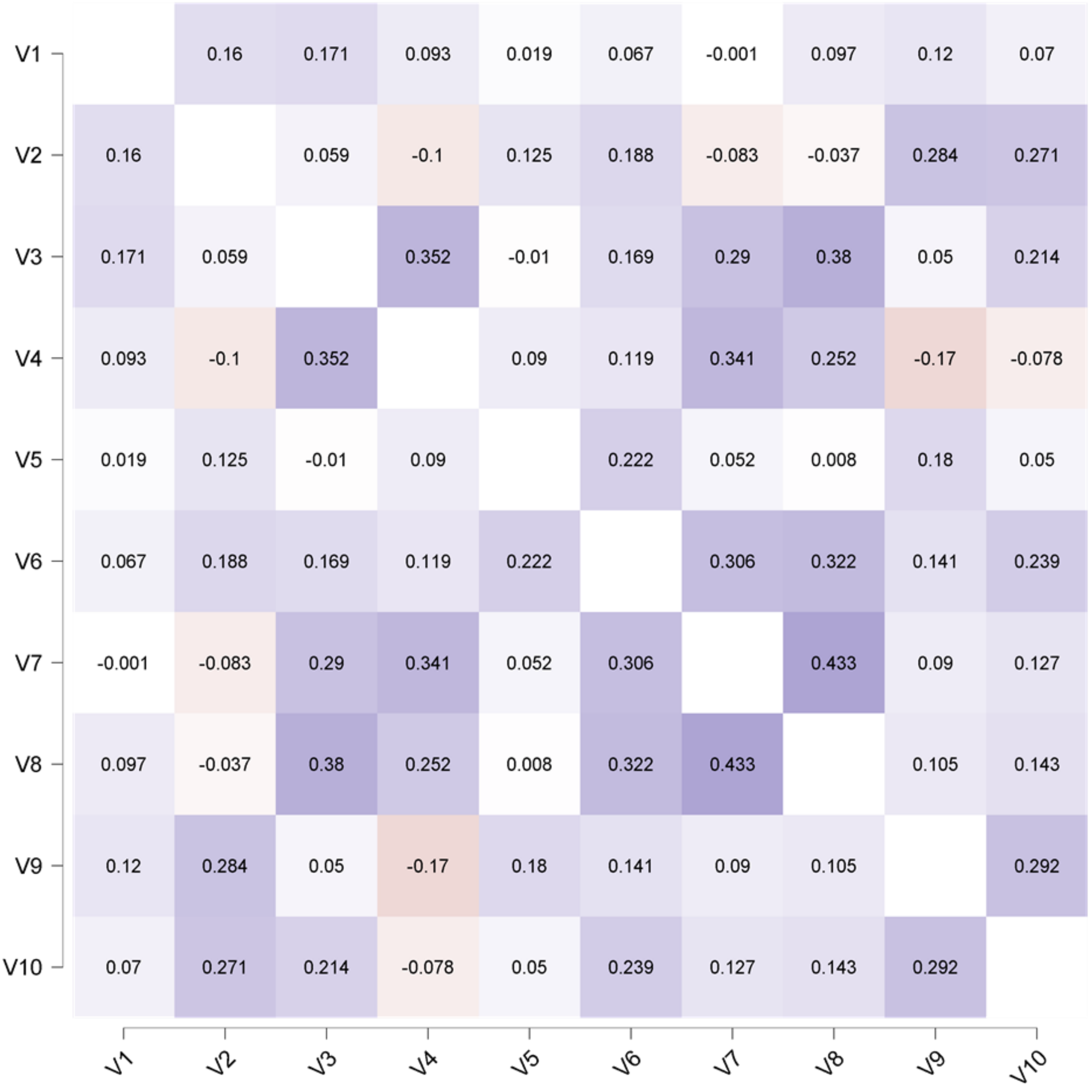
* p < .05, ** p < .01, *** p < .001 Determinant = 0.253

### TABLE 4: COMPONENT LOADINGS

| | PC1 | PC2 | PC3 | PC4 | UNIQUENESS |
|---|---|---|---|---|---|
| V1 | | | | 0.856 | 0.256 |
| V2 | | 0.608 | | | 0.45 |
| V3 | 0.633 | | | | 0.407 |
| V4 | 0.552 | -0.455 | | | 0.332 |
| V5 | | | 0.906 | | 0.174 |
| V6 | 0.478 | | | | 0.47 |
| V7 | 0.767 | | | | 0.378 |
| V8 | 0.76 | | | | 0.41 |
| V9 | | 0.693 | | | 0.489 |
| V10 | | 0.718 | | | 0.406 |

Note: Applied rotation method is varimax.

FIGURE 1: PEARSON'S CORRELATION HEATMAP



| | V1 | V2 | V3 | V4 | V5 | V6 | V7 | V8 | V9 | V10 |
|---|---|---|---|---|---|---|---|---|---|---|
| V1 | | 0.16 | 0.171 | 0.093 | 0.019 | 0.067 | -0.001 | 0.097 | 0.12 | 0.07 |
| V2 | 0.16 | | 0.059 | -0.1 | 0.125 | 0.188 | -0.083 | -0.037 | 0.284 | 0.271 |
| V3 | 0.171 | 0.059 | | 0.352 | -0.01 | 0.169 | 0.29 | 0.38 | 0.05 | 0.214 |
| V4 | 0.093 | -0.1 | 0.352 | | 0.09 | 0.119 | 0.341 | 0.252 | -0.17 | -0.078 |
| V5 | 0.019 | 0.125 | -0.01 | 0.09 | | 0.222 | 0.052 | 0.008 | 0.18 | 0.05 |
| V6 | 0.067 | 0.188 | 0.169 | 0.119 | 0.222 | | 0.306 | 0.322 | 0.141 | 0.239 |
| V7 | -0.001 | -0.083 | 0.29 | 0.341 | 0.052 | 0.306 | | 0.433 | 0.09 | 0.127 |
| V8 | 0.097 | -0.037 | 0.38 | 0.252 | 0.008 | 0.322 | 0.433 | | 0.105 | 0.143 |
| V9 | 0.12 | 0.284 | 0.05 | -0.17 | 0.18 | 0.141 | 0.09 | 0.105 | | 0.292 |
| V10 | 0.07 | 0.271 | 0.214 | -0.078 | 0.05 | 0.239 | 0.127 | 0.143 | 0.292 | |

TABLE 2: KMO AND BARTLETT'S TEST

| | | |
|---|---|---|
| **Kaiser-Meyer-Olkin (KMO) Test (Overall)** | | .673 |
| | | |
| **Bartlett's Test of Sphericity** | **Chi-Square** | 145.385 |
| | **Df** | 45 |
| | **Sig.** | < .001 |

Kaiser-Meyer-Olkin (KMO) test value is .673 i.e. more than .5, so acceptable according to table 2. Therefore, factor analysis is possible for these variables. In the same way factor analysis is suitable as per table 2, as the mentioned Bartlett's test significance value is < .001.

### b) Factor Extraction

There are 10 components in initial eigenvalues and 4 components after rotation. There is slight percentage difference between initial eigenvalues and after rotation as per table 3. Extraction Method used is Principal Component Analysis to get figures mentioned in the tables 3 and 4. At the initial stage, all components are treated equal and value 1 is given.

TABLE 3: TOTAL VARIANCE EXPLAINED

| | INITIAL EIGENVALUES | | | ROTATION SUMS OF SQUARED LOADINGS | | |
|---|---|---|---|---|---|---|
| | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % |
| 1 | 2.38 | 23.80% | 23.80% | 2.19 | 21.90% | 21.90% |
| 2 | 1.72 | 17.20% | 41.00% | 1.71 | 17.10% | 39.00% |
| 3 | 1.1 | 11.00% | 52.00% | 1.17 | 11.70% | 50.70% |
| 4 | 1.03 | 10.30% | 62.30% | 1.16 | 11.60% | 62.30% |
| 5 | 0.8 | 8.00% | 70.30% | | | |
| 6 | 0.76 | 7.60% | 77.90% | | | |
| 7 | 0.65 | 6.50% | 84.40% | | | |
| 8 | 0.6 | 6.00% | 90.40% | | | |
| 9 | 0.49 | 4.90% | 95.30% | | | |
| 10 | 0.47 | 4.70% | 100.00% | | | |

TABLE 5: COMPONENT CHARACTERISTICS

| | EIGENVALUE | PROPORTION VAR. | CUMULATIVE |
|---|---|---|---|
| PC1 | 2.382 | 0.238 | 0.238 |
| PC2 | 1.72 | 0.172 | 0.41 |
| PC3 | 1.1 | 0.11 | 0.52 |
| PC4 | 1.025 | 0.103 | 0.623 |

As per tables 4 and 5 as well as figures 2 plus 3, generated by the analysis software based on R has extracted 4 factors using varimax rotation method. The loadings less than .45 are suppressed in output. The four factors or component groups i.e. PC1/RC1 to PC4/RC4 are named below:

1) PC1/RC1 = Careless about security.
2) PC2/RC2 = Check and use online security features.
3) PC3/RC3 = Destroy mail after changing pin.
4) PC4/RC4 = Respond to messages for security purpose.

FIGURE 2: SCREEN PLOT

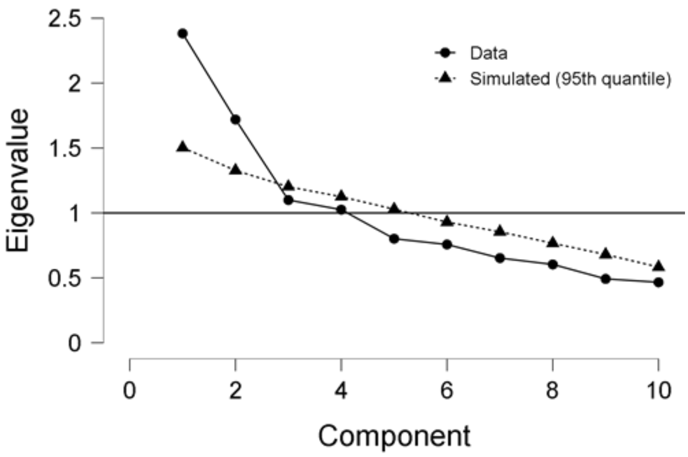
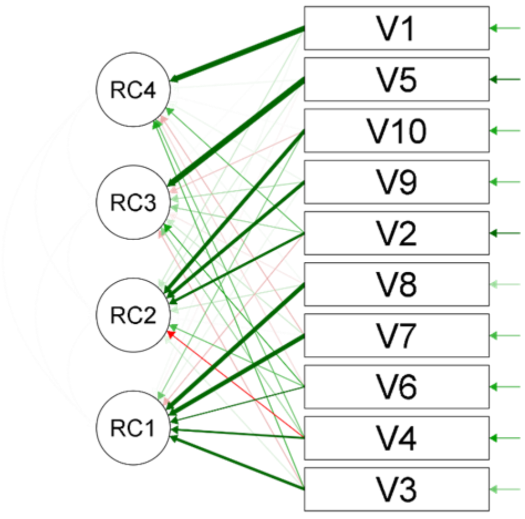


FIGURE 3: PATH DIAGRAM



## DISCUSSION:

The aim of the current study is to research future opportunities and challenges faced by digital healthcare sector. The qualitative analysis was undertaken to understand the problems faced by the same sector. They have reported many cybercrime cases worldwide. In case of India, also the number of cybercrime cases have risen over the years.

The quantitative analysis was also done to find out the present scenario of digital healthcare sector. The questionnaire was developed and primary data was collected. As per the results, the respondents were willing to provide information using mobile phones. They also wanted new laws to protect privacy on the internet. The cyber-attacks will have negative impact on privacy of patients. [16]

The secondary data related to Annual Global Healthcare Funding, Annual Global Corporate Funding for Digital Health, Annual Global Healthcare CyberSecurity Funding, Annual Global Cybersecurity Market and Number of Cyber Crime Cases Reported in India was also collected for hypotheses testing. The aim was to test the correlations between them. It is generally assumed that with the increase in funding for healthcare sector plus more corporate funding for digital health including increase in cybersecurity funding globally would reduce the number of cybercrime cases, but that is not happening. The cyber-attacks have increased during the current pandemic period. [17] The question arises then what should be done to bring down the number of cybercrime cases? The answer would help to overcome the challenges in digital healthcare sector.

The factor analysis was conducted on the ten statements regarding information security mentioned in the questionnaire. The respondents provided data that helped to know the security measures or precautions taken by them to protect the data and information from different types of cybercrimes. The four factors were extracted namely careless about security, check and use online security features, destroy mail after changing pin plus respond to messages for security purpose. The further research can be done based on the four mentioned factors. The war is between cyber security and crimes in digital healthcare sector, where cyber security will win only when the number of cybercrime cases would reduce.

### LIMITATIONS

The study is restricted to secondary and statistical data available up to 2020. The National Crime Records Bureau has provided data up to 2019 only. Sample size (111) of primary data is limited due to Covid pandemic, lack of time, resources and an on ongoing process.

### IMPLICATIONS

The healthcare industry has to safeguard the data by regularly monitoring the systems. As we upload more records and detailed personal data of people in the online system, the attackers would like to steal or hack the data. The healthcare sector has to develop Alert Intelligent Systems (AIS) to know whenever an attacker tries to attack the digital resources, so that the system can automatically counter. [18] They have to develop a business continuity and recovery plan plus report the same to cybercrime cell for further investigation. If attackers feel that they will be punished with imprisonment and or fine then only it will be a deterrent and help in reducing the number of cybercrime cases.

## CONCLUSION

The cybercrime cases have increased even after spending on cyber security measures. It is important to have security controls at all levels to protect personal information and medical records of people. It is important to create awareness among people about cyber security. Healthcare sector and government authorities have to do these on a consistent basis. It requires more research to be done and create a crime mapping to understand plus overcome the challenges.

## References

1. Edirippulige S, Senanayake B. Professional Practices for Digital Healthcare. Opportunities and Challenges in Digital Healthcare Innovation [Internet]. 2020 [cited 2021 April 11];97–112. Available from: https://www.igi-global.com/gateway/chapter/254968
2. Gercke, M. Understanding cybercrime: phenomena, challenges and legal response, ITU Telecommunication Development Bureau [Internet]. 2012 [cited 2021 April 25]. Available from: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime legislation EV6.pdf
3. CB Insights. App.cbinsights.com [Internet]. 2021 [cited 20 April 2021]. Available from: https://app.cbinsights.com/research/real-world-evidence-healthcare-media/
4. Sumant Ugalmugle, Rupali Swain. Digital Health Market Size By Technology [Tele-healthcare {Telecare (Activity Monitoring, Remote Medication Management), Telehealth (LTC Monitoring, Video Consultation)}, mHealth {Wearables (BP Monitors, Glucose Meter, Pulse Oximeter, Sleep Apnea Monitors, Neurological Monitors), Apps (Medical, Fitness)}, Health Analytics, Digital Health System (EHR, e-prescribing System)], By Component [Hardware, Software, Services], Industry Analysis Report, Regional Outlook, Application Potential, Price Trends, Competitive Market Share & Forecast, 2020 – 2026 [Internet]. Global Market Insights, Inc. Global Market Insights, Inc.; 2020 [cited 2021 April 20]. Available from: https://www.gminsights.com/industry-analysis/digital-health-market#:~:text=Digital%20Health%20Market%20size%20was,the%20digital%20health%20industry%20growth.
5. Siriwardhana Y, Gür G, Ylianttila M, Liyanage M. The role of 5G for digital healthcare against COVID-19 pandemic: Opportunities and challenges. ICT Express [Internet]. 2020 Nov [cited 2021 April 20]; Available from: https://www.sciencedirect.com/science/article/pii/S2405959520304744?via%3Dihub
6. Mukul. Patients' Privacy & Data Threat in Digital Era. eHealth Magazine [Internet]. Eletsonline.com. 2020 [cited 2021 April 12]. Available from: https://ehealth.eletsonline.com/2020/02/patients-privacy-data-threat-in-digital-era/amp/
7. Chernyshev M, Zeadally S, Baig Z. Healthcare Data Breaches: Implications for Digital Forensic Readiness. Journal of Medical Systems [Internet]. 2018 Nov 28 [cited 2021 April 29];43(1). Available from: https://link.springer.com/article/10.1007/s10916-018-1123-2#citeas
8. Lee D, Yoon SN. Application of Artificial Intelligence-Based Technologies in the Healthcare Industry: Opportunities and Challenges. International Journal of Environmental Research and Public Health [Internet]. 2021 Jan 1 [cited 2021 April 29];18(1):271. Available from: https://www.mdpi.com/1660-4601/18/1/271/htm
9. Dutta, P. 5 Biggest Cyber Attacks in India | Everything You Need to Know | Kratikal [Internet]. Kratikal Blog. 2019 [cited 2021 April 5]. Available from: https://www.kratikal.com/blog/5-biggest-cyber-attacks-in-india/
10. Significant Cyber Incidents | Center for Strategic and International Studies [Internet]. Csis.org. 2021 [cited 2021 April 15]. Available from: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
11. Application Security in the Rapid Digital Transformation Age: 2021 Threatscape [Internet]. @BrightTALK. 2021 [cited 2021 April 5]. Available from: https://www.brighttalk.com/webcast/17474/465278/application-security-in-the-rapid-digital-transformation-age-2021-threatscape
12. CB Insights. App.cbinsights.com [Internet]. 2021 [cited 20 April 2021]. Available from: https://app.cbinsights.com/research/report/industries-tech-shaping-world-post-covid/
13. Nithin Thomas Prasad. Corporate Funding for Solar Slid Globally in 1H 2020 But, It Could Have Been Worse - Mercom India [Internet]. Mercom India. 2020 [cited 2021 April 5]. Available from: https://mercomindia.com/corporate-funding-solar-slid-globally/
14. Crime In India | National Crime Records Bureau [Internet]. Ncrb.gov.in. 2020 [cited 2021 March 5]. Available from: https://ncrb.gov.in/en/crime-india
15. Field A. C8057 (Research Methods II): Factor Analysis on SPSS Factor Analysis Using SPSS [Internet].; [cited

2021 March 5]. Available from: http://www.discoveringstatistics.com/docs/factor.pdf

16. Mrcela M, Vuletic I. Healthcare, Privacy, Big Data and Cybercrime: which one is the weakest link? Annals of Health Law [Internet]. 2018 [cited 2021 August 30];27(2). Available from: https://lawecommons.luc.edu/annals/vol27/iss2/9
17. Lallie HS, Shepherd LA, Nurse J, Erola A, Epiphaniou G, Maple C, Bellekens X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security [Internet]. June 2021 [cited 2021 August 30];105. Available from: https://www.sciencedirect.com/science/article/pii/S0167404821000729
18. Guiora A. N. Cybersecurity: Geoplotics, law, and policy. London: Routledge, Taylor & Francis Group; 2017.