Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.776608

DATA PRIVACY AND SECURITY CHALLENGES IN AI-DRIVEN HEALTHCARE SYSTEMS IN INDIA

Sathish Kumar Chintala

Senior Engineer Ai And Ml Texas, Usa.

ABSTRACT

AI has become a transformative force in the Indian healthcare sector, offering numerous opportunities for cost, quality, efficiency, and accessibility. The integration of AI in administrative and clinical healthcare functions, including natural language processing, chatbots, computer vision, and machine learning, is exemplified by IBM's Watson and innovative startups. The government's initiatives, such as the National Health Protection Scheme, demonstrate the government's commitment to leveraging AI to enhance healthcare quality, accessibility, and affordability. However, the transformative potential of AI in healthcare is accompanied by significant challenges, primarily revolving around data privacy and security. The paper examines legal aspects, examining regulations like the National Medical Commission Act and Telemedicine Practice Guidelines, and scrutinizes government policies regulating health data. It also discusses the implications of cyber-attacks on telemedicine and the importance of data security in AI-driven healthcare. The paper also explores AI's role in reducing fraud in healthcare schemes, such as Ayushman Bharat, by implementing machine learning and facial recognition software. Challenges in the widespread adoption of AI include ethical concerns, legal uncertainties, infrastructure limitations, and information asymmetries.

INTRODUCTION

The Indian healthcare industry is rapidly adopting AI technology to address the shortage of skilled physicians and improve data quality in Electronic Health Records (EHR) data. AI has shown promising results in areas such as predictive modeling and predictive treatment. However, the development of AI for healthcare applications in India is still in its early stages, and a comprehensive healthcare policy is needed to address the complex challenges that have not yet been adequately addressed.

AI technologies can be classified into three broad categories: descriptive, predictive, and prescriptive. Descriptive AI helps in understanding past events, predictive AI anticipates future events, and prescriptive AI guides decision-making, suggesting potential therapies. AI can also augment human healthcare tasks, such as computer vision, natural language processing, speech recognition, and chatbots. The adoption of AI in Indian healthcare systems signifies a significant leap towards enhanced diagnostics, personalized treatment plans, and efficient resource allocation. AI applications, such as predictive analytics for disease outbreaks and image recognition in diagnostics, have the potential to revolutionize healthcare services in a country with a growing population. However, the nexus between AI, data privacy, and security becomes a critical focal point as India transitions into a digitally-driven healthcare ecosystem.

One of the primary challenges lies in safeguarding the privacy of health data, as patient records, diagnostic images, and genomic information are now digitized and susceptible to potential breaches. The ethical use and protection of this highly sensitive data become imperative to maintain public trust and comply with legal frameworks. India is grappling with the formulation of robust data protection laws, and there is a pressing need to scrutinize and fortify the regulatory framework governing AI in healthcare to ensure the highest standards of data privacy. The interconnectedness of healthcare networks and the integration of AI algorithms creates a vast attack surface susceptible to cyber threats. Cybersecurity breaches compromise patient confidentiality, jeopardize medical data integrity, and hinder the reliability of AI-assisted diagnoses. As India moves towards a Digital Health Mission and electronic health records implementation, the security of these systems becomes paramount.

Research Rationale:

This research paper aims to delve into the intricate dynamics of data privacy and security challenges in AI-driven healthcare systems in India. By addressing the vulnerabilities inherent in the convergence of AI and healthcare data, the research seeks to contribute to the formulation of informed policies, ethical guidelines, and technological safeguards. It endeavours to provide insights into the delicate balance between leveraging the potential of AI for improved healthcare outcomes and mitigating the associated risks to individual privacy and data integrity.

Through an in-depth analysis of existing regulatory frameworks, case studies of data breaches, and an exploration of international best practices, this research aspires to offer a comprehensive understanding of the current landscape. The findings aim to inform stakeholders, policymakers, and practitioners about the critical importance of proactively addressing data privacy and security concerns in the era of AI-driven healthcare in India.

AI IN HEALTHCARE

AI is a transformative innovation that will provide several advantages to the healthcare industry. AI has been quickly advancing in the domains of machines that possess the ability to see, understand, acquire knowledge, and perform administrative and clinical healthcare tasks.

AI exemplifies human intellect and is revolutionizing several industries, including healthcare. The use of AI has facilitated the realization of telemedicine and telesurgery, leading to a gradual transformation of the healthcare industry. There has been a substantial rise in the quantity of patents submitted in the healthcare industry throughout the last eight years. (Refer to figure 1).

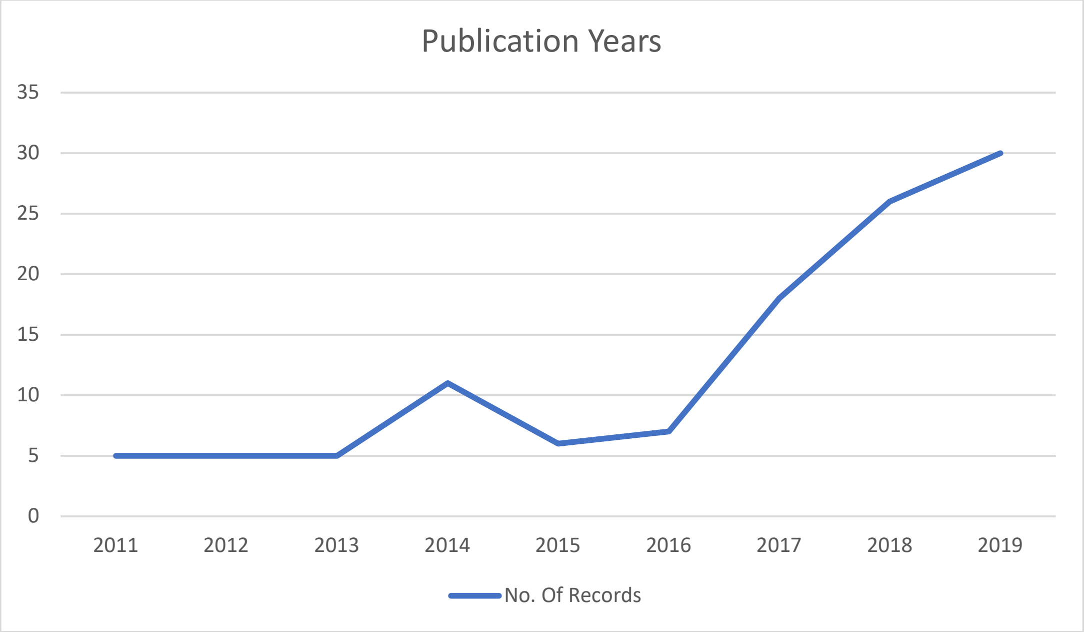

Figure 1: Worldwide Published Patents on AI and Healthcare (2011-19)

Artificial intelligence expands the range of tasks that robots are capable of doing, including natural language processing, chatbots, computer vision, and machine learning. Machine learning may be used to comprehend the vast amount of healthcare data and decrease the time required for decision-making. IBM's Watson is used in cancer operations to recommend the most appropriate therapy for patients. In India, there are emerging firms that use AI to tackle issues pertaining to the efficient delivery of services, automated diagnosis, illness detection and screening, as well as predictive healthcare diagnosis. Likewise, it will promote the elimination of biased therapies rooted in social or structural factors.[i]

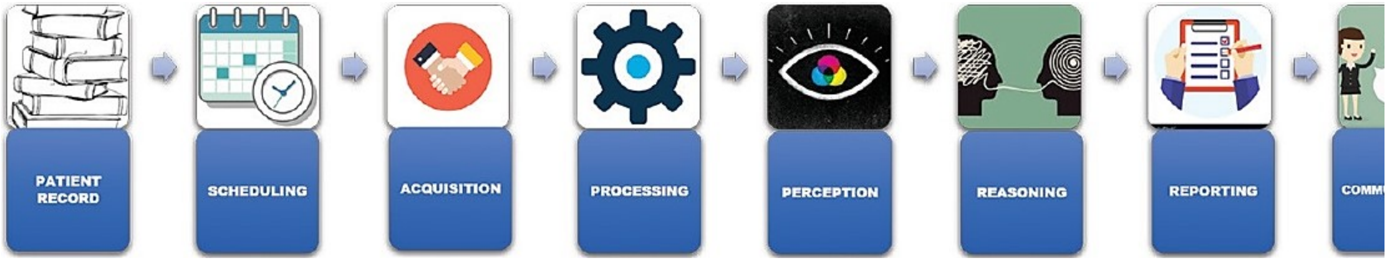

Figure 2: Flow of information in Artificial intelligence[ii]

The integration of AI in the healthcare business will significantly impact the cost, quality, efficiency, and accessibility of healthcare in underprivileged regions. The main emphasis is on delivering services to regions without infrastructure or where the quality of basic healthcare is uncertain. Nevertheless, the complete substitution of physicians and doctors with automation remains a subject of debate that will be addressed by society in the future. Conversely, the primary emphasis of AI's influence in India is centred on tackling economic inequality. The government has collaborated with its think tank, the “National Institution for Transforming India Aayog” (NITI Aayog), with Google to promote AI research, hence supporting the advancement of technology in New India. In addition, NITI Aayog is implementing a nationallevel analytical portal utilizing AI technology. The objective is to establish a centralized health record system for the “National Health Scheme” (NHS). This system will facilitate the efficient management of health information through the application of big data analytics and machine learning.[iii]

The Indian government is implementing steps to improve the influence of AI on healthcare, with the aim of improving the quality of healthcare services in rural areas of India. The Ayushman Bharat National Health Protection Scheme aimed to provide accessible and cost-effective healthcare services to every individual in the country. The healthcare scheme is the biggest in the world and focuses on managing strategic difficulties related to database maintenance and quality standards. The Indian government has used AI, deep learning, and machine learning techniques to address such circumstances.

DATA SECURITY AND TELEMEDICINE: A LEGAL PERSPECTIVE

According to the World Health Organization's (WHO) definition, telemedicine is the "delivery of health care services, where distance is a critical factor, by all health care professionals using information and communication technologies for the exchange of valid information for the diagnosis, treatment, and prevention of disease and injuries, research and evaluation, and for the continuing education of healthcare providers." Telemedicine is used to diagnose, treat, and prevent diseases and injuries, as well as for research and evaluation. The Netherlands laid the groundwork for contemporary telemedicine in the early 1900s by becoming the first country to transmit heart rhythms over the telephone. By the 1920s, this was already expanding to include transmissions to radio consultation centres located throughout Europe.[iv] Because of telemedicine programmes, the number of people hospitalised for mental health issues decreased by more than 40% in 2012, while the number of people hospitalised for heart failure decreased by 25%. The number of people hospitalised for diabetes and chronic obstructive pulmonary disease decreased by 20%. 6 In 2015, around 677,000 veterans had access to a total of approximately 2.1 million telehealth sessions.[v]

The integration of AI in telemedicine has led to both opportunities and challenges in the healthcare industry. As telemedicine grows, it provides remote access to medical consultations and diagnostics, but it also raises concerns about the privacy and security of patient data. The use of AI in telemedicine enhances healthcare systems by introducing advanced analytics, predictive modeling, and machine learning algorithms. These algorithms can analyze vast datasets, providing insights into disease patterns, treatment outcomes, and personalized healthcare recommendations. However, the use of AI also introduces additional layers of complexity to data security concerns. As AI algorithms learn and adapt, there is a constant exchange of information between systems, raising concerns about potential vulnerabilities in data security. Challenges such as unauthorized access, data breaches, and algorithmic biases necessitate a meticulous legal framework to address these issues. Legal frameworks like the Telemedicine Practice Guidelines play a crucial role in establishing standards for the secure transmission and storage of healthcare information.[vi]

Studies demonstrate that in the 1960s, the NASA, Lockheed Corporation, and the United States Indian Health Service worked together to construct the “Space Technology Applied to Rural Papago Advanced Health Care” (STARPAHC) project, which was a significant turning point in the development of telemedicine. Telemedicine programmes on a massive scale, such as STARPAHC, are now in the process of being created. A member of the medical community was able to provide telemedicine services to a Native American tribe by using the same equipment that was designed specifically for use by astronauts when they were in orbit. Telemedicine is reportedly used in several programmes that get funding from either the government or grants, including:[vii]

- Delivering healthcare services in a conflict-ridden area.
- Delivering healthcare services to isolated research outposts located in the Arctic and Antarctic regions.
- Delivering healthcare services to correctional institutions without the need to transfer convicts to a hospital.
- Transmission of radiological pictures using digital technology.

GOVERNMENT POLICIES REGULATING HEALTH DATA

The government of India is making strenuous efforts to establish a centralised healthcare system, with the intention of one day digitally recording the medical records of each Indian person. The implementation of the National Health Policy, 2017, which was the first step toward achieving the policy's stated goal of providing citizens with access to high-quality medical care through the development of a national digital health ecosystem ("NDHE"), was the first step in realising the policy's stated objective. Since then, both the Ministry of Health and the NITI Aayog, which is the think tank of the Indian government, have given their sets of instructions for the establishment of the NDHE. These regulations, which comprise the National Health Stack and the National Digital Health Blueprint Report, describe the core architecture and structure of the NDHM. The NDHM, a critical digital health initiative, will get off the ground on August 15, 2020, according to an announcement made by India's government. Every person who resides in India is going to be given a Health ID as part of the NDHM's plan. The “National Data Health Model” (NDHM), which includes the Health Data Management Policy, was recently released for public study and comment. Patients, healthcare practitioners, clinical institutions, pharmaceutical firms, insurance providers, and others all have responsibilities and rights that are spelt out in the HDM Policy, which addresses data protection and privacy concerns related to health data.[viii]

QUALITY AND SECURITY OF DATA

Ayushman Bharat is highly dependent on the appropriate management of data, which is crucial for its progress. Data privacy is a pressing concern that requires attention as it ensures the protection of patient stakeholders, service providers, and others involved. The data must adhere to certain principles, including collection, storage, completeness, and interchange, in order to establish a sound framework that guarantees the reliability and acceptability of the data. One difficulty experienced by patients is the inaccessibility of their medical data owing to a lack of a good system. As a result, they are unable to provide the essential evidence to another specialist, which may be inconvenient during crises. The second difficulty pertains to the securitization of data, which involves guaranteeing the security and privacy of data during its storage, standardization, and sharing between various bodies.[ix] Currently, service providers are required to comply with the Information Technology Rules, 2011, which protect the collection, reception, storage, and transfer of sensitive information. These rules are established under the Information Technology Act 2000. Effective management of information and data exchanged between hospitals, diagnostics facilities, and clinics is essential. Both obstacles may be overcome by using deep learning techniques. In hospitals, the use of diverse software ensures the security and easy accessibility to data and information. Likewise, IT leaders may facilitate the exchange of information across hospitals and authorities using programming languages like R and Python.[x]

REDUCING FRAUDS

Annually, a staggering amount of US$260 billion (5.59% of global healthcare expenditure) is wasted worldwide due to fraudulent activities. The lack of consistent information provided by subordinates in government-organized healthcare schemes, insurance plans, and programs results in fraudulent actions inside the whole system. This leads to instances of misconduct, compelling requests from providers, fraudulent policyholders, counterfeit beneficiaries, and similar occurrences. To combat these unethical practices in Ayushman Bharat, a framework has been established under the Anti-fraud Guidelines, 2018. The primary objective of this framework is to identify, prevent, and discourage fraudulent and abusive behaviours inside the system.

The Indian government has used AI as an additional safeguard to oversee patterns and establish standardized treatment procedures in order to prevent anomalies such as excessive invoicing or charging, unnecessary testing, incorrect beneficiary information, and misuse of the referral system. The program reached about 300,000 recipients in 10 months. The Government has enlisted the National Health Authority (NHA) to combat fraudulent activities in the program. The NHA diligently identifies such scams and conducts thorough investigations before implementing any actions against them (National Health Authority, 2018).

The National Health Authority (NHA) identified irregularities in 48 hospitals nationwide, resulting in the suspension of 31 institutions. The suspensions were imposed for various reasons.

- Inconsistencies in doctors' availability throughout working hours at public hospitals.
- Doctors at public hospitals are engaging in the unlawful practice of sending their patients to private hospitals in exchange for financial incentives by issuing referral slips.
- Transferring patients from private clinics to private hospitals.
- Hospitals manipulated data pertaining to a provision within the program, which stipulated that a patient would be eligible for payments if they were hospitalized for a minimum of 6 hours.

Due to these inconsistencies, the NHA developed an IT system utilizing machine learning to enable hospitals and diagnostics centres to access up-to-date information. This includes beneficiary identification, fund flows, transaction management, claims payment, and details of referred patients, among other activities. Through the use of this system, the NHA enforces strictness in order to exert control on insurance firms, both commercial and public hospitals, and to ensure the efficient allocation of healthcare benefits to the recipients. By specifying specific characteristics that outline fraudulent actions and incorporating advanced face and speech recognition software into CCTV cameras, AI has the potential to detect potential frauds effectively.

CHALLENGES

India has several prospects for the use of AI; however, it is essential to address the first obstacles associated with technology management. Firstly, it is essential to address the ethical ramifications of using artificial intelligence in the healthcare sector. Additionally, we should explore potential solutions to tackle these issues effectively. AI will encounter four primary ethical challenges: prejudice, lack of awareness, lack of data privacy, and singularity - the phenomenon of AI intellect surpassing that of humans. The primary approach to address these challenges is to ensure that the backend programming and data implementation are adaptable enough to accommodate software engineers from diverse socio-cultural backgrounds. Additionally, the utilization of reinforcement learning in AI, which involves learning through trial and error to achieve specific goals, is crucial.[xi]

Effective advancement can only occur when a solid and comprehensive legal structure is established. Several obstacles include the control of power within institutions, the need for suitable certification processes, infrastructural requirements, economic investment, unresolved legal issues, and information imbalances and views. India currently does not have a regulatory authority to oversee the effect of AI in the healthcare industry and ensure data security to avoid abuse of data. India lacks the necessary infrastructure to conduct cost-effective clinical trials, leading to prolonged timelines and a lack of standardized quality certifications, which renders the collected data unreliable. Hence, a potential resolution might include including physicians as panel members throughout the implementation of AI in the field.

Implementing AI in India is a significant difficulty due to the lack of necessary infrastructure, such as sufficient cloud computing resources, high-speed internet, and processing power. These essential components are still largely lacking in many areas of the nation, resulting in the need to host servers overseas. Moreover, the public sector in India provides little funding for AI, resulting in its present restriction to a small number of professional domains.

Concerns arise in the domain of information asymmetries and perceptions since physicians and coders lack clear standards to ensure consistency. Consequently, they exhibit reluctance to adopt new software and adapt it to their use. Furthermore, there is a dearth of comprehension about the necessary regulations, terms, and circumstances for utilizing such technology, as well as a substantial number of unresolved legal inquiries that will establish accountability in the event of any mistakes made by the associated pros. Hence, it is crucial to explicitly define specific guidelines and protocols that align with the specific situations and working conditions.

The influence of AI on big data in research has been steadily increasing in recent years. This is evident via the advancements in chatbots, individualized clinical diagnosis, and improved accuracy in illness prediction. These developments have made a clear distinction between conventional IT and AI. Several hospitals in India have directly experienced the use of descriptive and predictive artificial intelligence. Manipal Group of Hospitals used technology breakthroughs, namely IBM Watson, to assist physicians in delivering precise therapies to cancer patients within their oncology focus.[xii]

Aravind Eye Care utilizes AI to evaluate gathered data for early diagnosis of ailments like diabetes and blood pressure. AI may be advantageous in the pharmaceutical business by improving the value proposition, automating sales processes, and distinguishing products in the market. Pharmarack employs AI in its supply chain to guarantee optimal efficiency.

Startups and multinational corporations (MNCs) are using AI in the domain of diagnostics to discover and diagnose diseases at an early stage. This includes companies like Google and IBM. In addition, some firms are using deep learning and machine learning techniques to identify first symptoms and suggest tailored treatment measures. Within the realm of startups, notable examples include Cureskin, which specializes in addressing skin ailments such as scars, pimples, and warts, and Qure.ai, which uses deep learning to facilitate timely identification and subsequent medical interventions.

AI is very beneficial in the field of counselling psychology. In Indian civilization, depression is often seen as a social shame. Therefore, artificial intelligence aids in the provision of chatbots (such as Wysa) that provide sympathetic assistance and recommend seeking advice from human professionals. Anonymity is a crucial element in this scenario as it enables patients to express their emotions without fear of judgment or categorization.

Additionally, telemedicine facilitates the delivery of high-quality and cost-effective healthcare services in rural areas of India, while AI eliminates any discrimination among the population. An instance of commercial activity in this domain is SigTuple, an Indian company that examines blood samples and produces reports autonomously, without the assistance of pathologists. Philips Innovation Campus (PIC) is an exemplary case that has made healthcare more inexpensive and accessible via the use of AI. Philips, in collaboration with Fortis Escorts Heart Institute in Delhi, has developed IntelliSpace Consultative Critical Care, a system that enables the centralized monitoring of several critical care units.[xiii]

CONCLUSION

Ultimately, artificial intelligence in Indian healthcare promises enormous improvements in efficiency, accessibility, and quality. This detailed exploration shows that AI technologies like natural language processing, machine learning, and computer vision could transform healthcare delivery, especially in diverse and populous India.

AI, deep learning, and machine learning help Ayushman Bharat, the world's largest healthcare plan, solve strategic management problems. The government's vision of a technology-empowered New India includes using AI to reduce economic gaps and improve rural health care.

This technology revolution has obstacles, and our analysis has raised important issues. AI-driven healthcare systems make data privacy and security top priorities. Telemedicine systems may be vulnerable to cyberattacks, highlighting the need for strong laws, ethics, and security. The National Medical Commission Act, Telemedicine Practice Guidelines, and other government standards protect data, but they must be updated to keep up with AI.

AI can reduce healthcare fraud, and machine learning and facial recognition can protect systems like Ayushman Bharat, according to the study. AI solves problems, but ethical issues, legal difficulties, infrastructure constraints, and knowledge asymmetries prevent its wider use. A diversified approach is needed to overcome these limitations and maximize AI in healthcare. Establishing a strong legal and ethical framework and updating it to accommodate new technologies is essential. Responsible AI deployment that prioritizes patient privacy, data security, and ethics requires collaboration between legislators, healthcare practitioners, and technological experts.

To bridge the digital gap and integrate AI across varied healthcare settings in India, technology and trained professional infrastructure investments are necessary. Interdisciplinary collaboration, such as doctors on AI deployment panels, can help close comprehension and acceptance gaps.

Finally, technology, ethics, and policy will shape Indian healthcare. AI could make healthcare more accessible, efficient, and egalitarian for India's varied population if managed well. As we enter this technological renaissance, AI in healthcare must be approached with a balanced viewpoint, appreciating its revolutionary capacity while prioritizing ethical and legal considerations.

REFERENCES

[i] Mahajan, Abhishek, Tanvi Vaidya, Anurag Gupta, Swapnil Rane, and Sudeep Gupta. "Artificial intelligence in healthcare in developing nations: The beginning of a transformative journey." Cancer Research, Statistics, and Treatment 2, no. 2 (2019): 182-189.

[ii] Mahajan, “Artificial intelligence in healthcare in developing nations: The beginning of a transformative journey.” Cancer Research, Statistics, and Treatment 2(2): p 182-189, Jul–Dec 2019. | DOI: 10.4103/CRST.CRST_50_19

[iii] Bajpai, Nirupam, and Manisha Wadhwa. “Artificial Intelligence and Healthcare in India.” No. 43. ICT India Working Paper, (2021).

[iv] Dossetor, J.B. “Beyond the Hippocratic Oath: A Memoire on the Rise of Modern Medical Ethics. Canada:” The University of Alberta Press, 301 p (2005)

[v] Ferrer-Roca, O. and Sosa-Iudicissa, “Handbook of Telemedicine (Third printing). The Netherlands: IOS Press”, 297 p. (2002)

[vi] *Vijai, C., and Worakamol Wisetsri. "Rise of artificial intelligence in healthcare startups in India." Advances In Management 14, no. 1 (2021): 48-52.*

[vii] *Ibid*

[viii] Chaudhuri, Ranjan, Sheshadri Chatterjee, and Demetris Vrontis. "Antecedents of privacy concerns and online information disclosure: Moderating role of government regulation." EuroMed Journal of Business 18, no. 3 (2023): 467-486.

[ix] Bradford, Laura, Mateo Aboy, and Kathleen Liddell. "COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes." *Journal of Law and the Biosciences* 7, no. 1 (2020): lsaa034.

[x] Nittari, Giulio, Ravjyot Khuman, Simone Baldoni, Graziano Pallotta, Gopi Battineni, Ascanio Sirignano, Francesco Amenta, and Giovanna Ricci. "Telemedicine practice: review of the current ethical and legal challenges." *Telemedicine and e-Health* 26, no. 12 (2020): 1427-1437.

[xi] Yaqoob, Ibrar, Khaled Salah, Raja Jayaraman, and Yousof Al-Hammadi. "Blockchain for healthcare data management: opportunities, challenges, and future recommendations." *Neural Computing and Applications* (2021): 1-16.

[xii] Pandey, Neena, and Abhipsa Pal. "Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice." *International journal of information management* 55 (2020): 102171.

[xiii] Vijai, C., and Worakamol Wisetsri. "Rise of artificial intelligence in healthcare startups in India." *Advances In Management* 14, no. 1 (2021): 48-52.