"EMERGING TRENDS IN THE DIGITAL WORLD"
HEALTH CARE SECTOR IN THE DIGITAL ERA

TARUN.M[1]

S.SAINDHAVI[2]

Abstract

The digital health sector has opened up as a critical solution to bridge the gap and challenges in the delivery of quality health care. Advances in Healthcare Artificial Intelligence are growing rapidly and there is a heated discussion about managing its development. While governments and medical companies have long been the main investors, big tech companies including Google, Microsoft have started to invest more in digital health. Additionally, with the unprecedented COVID-19 pandemic around the world, discussions about digital health are resurfacing. This has resulted in a major shift in digital health focus areas as new technologies emerge and regulations evolve due to the combined expertise. Yet they also pose privacy and confidentiality issues. In this paper, we will look into the various emerging technologies in the healthcare sector i.e.: telemedicine, artificial intelligence, etc., and the privacy issues faced in the technologies that evolved recently. This paper analyses the legislation and amendments in the health sector and the challenges faced in the digital era, especially the right to privacy and examines the current and existing legal framework to protect the right to health in India. This article also outlines the human rights violation due to breach of privacy and other mitigating risks due to the emerging digital technologies. It also covers the intellectual property rights being dealt with in the healthcare sector and also how alternative dispute resolution mechanisms evolved in digital health care.

1 School of Excellence in Law,
2 School of Excellence in Law

INTRODUCTION :

"The hare of science and technology lurches ahead. The tortoise of the law ambles slowly behind"

The healthcare industry is one of the fastest-growing industries in recent years. It constitutes over 10% of GDP (Gross Domestic Product) to our country's economy. The healthcare industry involves a number of key players like medical practitioners, patients, diagnostic labs, pharmacies. The growing population is pressuring the system to make a digital transformation in the healthcare industry. At the same time, patient engagement has been repeatedly

linked to better health outcomes. [1]Digital health may, for example, help patients self-screen; encourage conduct change; further develop cognizance of diagnosis and discharge plans; and licence dynamic trades between patients, their health care information, and doctors. Digital health tools have been hailed as easily disseminated, low-resource solutions to help patients take ownership of their healthcare journey.[2]

New wellbeing advances like wearable tech, telemedicine, genomics, virtual reality (VR), advanced mechanics and robots, artificial intelligence (Man-made intelligence) are changing the scene of the Indian medical services framework. In the same way as other different business sectors, India also is at the cusp of a 'Digital health revolution'

What is Digital Health?

There is a preferred tendency to group every technological advancement in healthcare that often comes within the purview of "Digital Health". But what exactly is Digital Health? The globe Health Organisation defines digital health as "a broad umbrella term encompassing eHealth, further as emerging areas, like the utilisation of advanced computing sciences in 'big data', genomics and artificial intelligence". Therefore, the expression Digital Health could also be said to incorporate the tools and services that use information and communication technologies (ICT) for purposes connected to health. These purposes may include improving accuracy of diagnosis, monitoring chronic diseases more closely and improving treatment outcomes for patients.

[1]Marks R, Allengrante JP, Lorig K. A review and synthesis of research evidence for self-efficacy-enhancing interventions for reducing chronic disability: implications for health education practice (part I) *Health Promot Pract.* 2005;6(1):37–43. [PubMed] [Google Scholar]
[2]Topol E. *The patient will see you now: The future of medicine is in your hands.* New York City, NY: Basic Books; 2015.

Technology is profoundly changing the way health care is delivered. Whether it is patients consulting general practitioners through online primary care services, the use of clinically applicable artificial intelligence and deep learning in diagnostic and referral pathways, or the robot-assisted surgery practised across continents, rapid technological development is transforming the healthcare landscape and it follows that the law must keep pace with these changes, especially in cases of accident or negligence and when liability issues arise. Are these laws sufficient to meet the challenges they pose? The reality is that accountability in the digital age is an emerging field with many complex facets. It is a challenge for legal regimes to evolve at a sufficient pace, but ultimately lawmakers and courts will need to ensure a fair distribution of losses, consistency of law and effective access to justice - the complexity and blurred lines of responsibility should not result in victims not being compensated for their losses.[3]

Telehealth, telemedicine, and eHealth are very general terms but their sole purpose is to provide healthcare to people who are far away. Patients through technologies that enable real-time, two-way interactive communication between patients and doctors. Telehealth is seen as an alternative to traditional face-to-face health care delivery. Telehealth is defined
such as "the use of information technology and electronic communications to support and promote health care, patient and professional education, public health and health administration ". Common telehealth applications include Live (synchronous) and Store and Forward (asynchronous) video conferencing, remote patient monitoring (RPM) and mobile health (mHealth). WHO (2009) 18 adopted a broader description of telehealth as "the delivery of health services, where distance is a critical factor, by all healthcare professionals using

[3]https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/strategic-principles-for-competing-in-the-digital-age

information and communication technologies for the exchange of valid diagnostic information, treatment and prevention of disease and injury, research and evaluation, and for continuing education in health care providers, all in the interest of advancing the health of individuals and their communities "? Telehealth differs from Telemedicine which offers more than clinical care services and takes several forms, such as teleconsultation, primary care, teleradiology, tele neurology, tele pharmacy, telepsychiatry, tele dermatology and virtually all disciplines health care, including telerobotic surgery. The main advantages of telehealth for patients are the absence of the need and cost of transport, savings in travel and waiting times, rapid access to health services and elimination of rural barriers; for service providers, these include lower practice costs and reduced practice overheads, and payers benefit in terms of quick access to health care with long term savings as disease escalation. Despite these advantages, barriers to telehealth include limited reimbursement, limited research showing telehealth benefits and return on investment, limited availability of high-speed telecommunications in remote areas, lack of capacity for high-resolution medical images, lack of standards and certification bodies, fear of malpractice, ethical and legal challenges, sustainability and state licensing problems.

EMERGING TECHNOLOGIES IN DIGITAL HEALTHCARE

ARTIFICIAL INTELLIGENCE :

Artificial intelligence (AI) and related technologies are increasingly prevalent in business and society, and are beginning to be applied in healthcare. These technologies have the potential to transform many aspects of patient care, as well as administrative processes within provider, payer and pharmacy organisations.

There are already a number of research studies suggesting that AI can perform as well or better than humans at key health tasks, such as diagnosing disease. Today, algorithms are already surpassing radiologists in spotting malignant tumours and guiding researchers in building cohorts for expensive clinical trials. However, for various reasons, we believe it will be many years before AI replaces humans for large areas of medical processes. In this article, we describe both the potential that AI offers to automate some aspects of care and some of the barriers to the rapid implementation of AI in healthcare.[4]

A survey conducted by a software company namely Mckinsey has submitted a report that looks at 23 apps in use today and provides case studies of 14 apps already in use. These illustrate the full range of areas where AI can have an impact: from apps that help patients manage their own care, to online symptom checkers and electronic e-triage AI tools, to virtual agent machines that can perform tasks in hospitals, and the bionic pancreas to help diabetic patients. Some of these helps to improve the health care operations by optimising schedules or bed management, others by predicting the risk of hospitalisation or helping to detect specific cancers early by allowing intervention that can lead to better survival rates, and others even help to optimise R&D and pharmacovigilance in the health sector. The scale of many solutions remains negligible , but their increasing adoption at the healthcare system level indicates that the pace of change is accelerating. In most cases, there isn't much research on whether AI can have an impact, but rather how to increase and expand its potential for impact to make it user friendly.[5]

[4] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6616181/

[5]https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/transforming-healthcare-with-ai

The biggest problem with handling robots is security and privacy concerns and power consumption. Artificial intelligence (AI) is the ability of computers to perform tasks commonly associated with human intelligence. However, collecting, storing and communicating a wide variety of personal patient data presents a major challenge. How to provide the data required by these new avenues of care while protecting the privacy of patients?

The following are the challenges regarding AI tools, which may hamper their widespread adoption:

- Data access: Developers struggle to get the high-quality data needed to build effective AI tools. Limitations and biases in the data used to develop AI tools can compromise on patients' privacy and their safety and effectiveness for different patient groups, leading to treatment disparities.

- Scaling and Integration: AI tools can be difficult to scale and integrate into new contexts due to differences between institutions and patient populations.

- Lack of transparency: AI tools sometimes lack transparency, in part because of the inherent difficulty in determining the working of the machines but also because of more controllable factors, such as the paucity of clinical assessments.

- Privacy: As more AI systems are developed, large amounts of patient's health data will be stored in the systems which poses a high risk of getting hacked increasing privacy risks and concerns.

- Uncertainty over liability: The multiplicity of parties involved in the development, deployment, and use of AI tools is one of the main factors that have made the liability associated with the use of AI tools uncertain. This can slow adoption and hamper innovation.[6]

AI is also used for vaccine development, thermal screening, CT scans, etc. AI-based systems are also regulated by the National Medical Commission Act, 2019t, Indian Medical Council Regulations, Medical Device Rules, 2017, IT Law, and Privacy Rules. India is home to several accredited multi-specialty hospitals and patient care centres, which are equipped with sophisticated technologies. With the increasing role of robotic surgeries and AI in healthcare in India, the Insurance Regulatory and Development Authority of India (IRDAI) released the standard individual health insurance product guidelines in January. 2020, ordering insurers to cover robotic surgeries under standard health insurance policies.

ELECTRONIC HEALTH RECORDS (EHR):

An electronic health record (EHR) is an electronic version of a patient's medical history, which is maintained by the provider over time, and can include all key administrative clinical data relevant to that person's care under a provider. EHR automates access to information, particularly demographics, progress notes, problems, medications, vital signs, medical history, vaccinations, lab data, and radiology reports and has the potential to streamline the workflow of the clinician. The EHR also has the ability to directly or indirectly support other care-related activities through various interfaces, including evidence-based decision support, quality management, and outcome reporting.

[6] https://www.gao.gov/products/gao-21-7sp

EHRs are the next step in the continued advancement of healthcare that can strengthen the relationship between patients and clinicians. The data with its timeline and availability, will enable providers to make informed decisions and provide proper care.

For example, the EHR can improve patient care by:

- Reduce the incidence of medical errors by improving the accuracy and clarity of medical records.
- Make health information available, reduce duplication of tests, reduce treatment delays, and educate patients to make better decisions.
- Reduce medical errors by improving the accuracy and clarity of medical records.

Digital health data records allow physicians to easily access a patient's medical history and make relevant consultations and recommendations - all efficiently and quickly. Digital health records also eliminate duplication of testing and dramatically reduce costs. Many private multi-specialty and super-specialty hospitals in India maintain EHR databases; however, most public hospitals are yet to upgrade their systems.

The MoHFW[7] initially notified the Electronic Health Record (EHR) Standards,2013 and also revised these standards in December 2016. All EHR technologies must comply with EHR standards. These EHR standards are largely based on the data protection principles set out in the privacy rules. More recently, the Indian state of Kerala successfully deployed an effective EHR system, collecting and storing electronic health records of over 25.8 million people as part of its eHealth project. This initiative allowed patients to go to any

[7] Ministry of Health and Family Welfare

public hospital without having to carry paper files. With the growing demand for contactless procedures, especially since the onset of the pandemic, several state governments are adopting these EHR systems and other such digital mechanisms for maintaining health records.

PRIVACY AND CONFIDENTIALITY IN EHR:

Judge Samuel Dennis Warren and Judge Louis Brandeis define privacy as the right "to be left alone".[8] The right of individuals to be left alone, from the surveillance or interference of other individuals, organisations, or even the government. A patient's information should only be disclosed to others with the patient's permission or permitted by law.[9]When a patient is unable to do so due to age, mental disability, decisions regarding information sharing should be made by the patient's legal representative or guardian. Information shared as a result of a clinical interaction is considered confidential and should be protected.[10] Information from which the identity of the patient cannot be established, for example, the number of patients with breast cancer in a public hospital, does not fall into this category.

Healthcare institutions, insurance companies, and others will need access to the data if EHRs are to function as intended. The key to maintaining confidentiality is to allow only authorised persons to have access to information. It starts with user authorization. User access is based on pre-established role-based privileges. The administrator identifies the user, determines the level of information to be shared, and assigns usernames and passwords. The user must be aware that he

[8]Warren SD, Brandeis LD. The right to privacy. *Harv Law Rev.* 1890;4:193. [Google Scholar] [Ref list]
[9]Rognehaugh R. *The Health Information Technology Dictionary.* Gaithersburg, MD: Aspen; 1999. p. 125. [Google Scholar] [Ref list]
[10] Rinehart-Thompson LA, Harman LB. Privacy and confidentiality. In: Harman LB, editor. Ethical Challenges in the Management of Health Information. 2nd ed. Sudbury, MA: Jones and Bartlett; 2006. p. 53. [Google Scholar] [Ref list]

will be responsible for the use and misuse of the information he consults. They have access to the information that they need to fulfil their responsibilities. Therefore, the assignment of user privileges is a major aspect of health record security. While controlling access to health information is important, it is not sufficient to protect confidentiality. Additional security measures such as strict privacy and security policies are essential to secure patient information.

TELEMEDICINE:

Telemedicine is the use of telecommunications technology to provide health care. While

Telemedicine is not a specialty in its own right, it's peculiarity is that various technologies are used in the delivery of traditional health services. It is a broad concept that covers in its address various aspects such as teleradiology, teleconsultation, telecare, and telesurgery.

Telemedicine has been introduced in India accounting for the use of various information and communication tools for health services, with the virtual presence of both patients and doctors. Telemedicine includes the tools used to perform technology-based patient consultation communication via video, audio, and text. Although telemedicine has been used in India for some time, the coronavirus pandemic has given telemedicine a significant boost. A survey by Practo, a popular Indian health technology company, recently estimated that there had been a 67% drop-in clinic visits and a massive 500% growth in online medical consultations just between the 1st. March 2020 and May 31, 2020.

Regarding the regulatory framework, India's Ministry of Health and Family Welfare (MoHFW) introduced the Guidelines for the Practice of Telemedicine (TPG) in March 2020. TGPs were introduced to help physicians to follow a

strong course of action in providing safe and effective care and fast online medical care. TGPs prescribe rules relating to the doctor-patient relationship, issues of liability and neglect, assessment, management and treatment, informed consent, continuity of care, referral to services emergency, medical records, confidentiality and security of patient records, and information exchange, prescription, and reimbursement, health education, and counselling. TGPs apply to registered physicians (i.e., who are listed in the State Medical Register or Indian Medical Register under the old Indian Medical Council Act 1956 and the current Act on the 2019 National Medical Commission (NMC law)). Under the current framework, TGP does not apply to licensed physicians outside of India.

With multiple lockdowns and movement restrictions across the country, healthcare workers and doctors used telemedicine solutions to provide increasingly rapid access to patients, as it was cost effective and could significantly reduce the associated pressure. to patients. Telemedicine Plays an important role when patients do not need to go to the hospital or to a doctor in person. The advancement of telecommunication technologies in India has improved the way a patient's medical history records are kept and can help patients better manage their medications and illnesses.

During last year's nationwide lockdown, when patients were forced to stay at home, healthcare professionals began providing remote consultations using video / audio calls and text messages . During the lockdown, technology-based consultations were also extended to COVID-19 patients with mild symptoms and for whom hospitalization was not required.

Additionally, there has been an increase in mental health issues during the lockdown due to the unprecedented Covid-19 pandemic. In this regard, health organizations and doctors offer online advice to people.

Besides this, various efforts have been made to promote telehealth in India. India Virtual Hospital, a medical technology service , has launched a patient care app that allows doctors to periodically monitor patients' health and recovery. Another healthcare technology company has recently launched an online platform, iCliniq, where users can get medical advice from doctors/practitioners, doctors, in the US, UK, United Arab, India, Singapore, Germany, etc. via emails, chats, video, and audio calls. Indian company set up a virtual hospital for cancer patients in 2019 via online consultation, treatment planning, and management of treatment.

The advancement of digital health technology has helped alleviate a variety of issues in the healthcare industry, ranging from diagnostic testing to promoting treatment. For the first time in India, the Indian Council of Medical Research (ICMR) has recently approved a COVID-19 self-test kit, called CoviSelf TM COVID-19 Rapid Antigen Self-Test Kit, which allows users to perform COVID-19 tests at home and get results in 20 minutes, via a mobile app. However, the CoviSelfTM mobile application has not yet been launched in India. Therefore, many specific aspects of the application, such as (i)how these service providers will handle patient health data, patient personal data, (ii)its legal consequences in the event of inaccurate results, (ii)how the provider will compensate users in case inaccurate results, (iv)and the number of damages in such cases, etc., have yet to be resolved.

Telemedicine platforms are currently governed by the NMC Act, the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002 (IMC Regulations), the Drugs & Cosmetics Act, 1940 (D&C Act), the Drugs & Cosmetic Rules 1945 (D&C Rules), the Clinical Facilities (Registration and Regulation) Act 2010, the Information Technology Act 2000 (Information

Technology Act), and the Computing Technology Rules 2011. information (reasonable security practises and procedures and sensitive personal data or information) (confidentiality rules).[11]

Also, in case of medical negligence, a patient can file a complaint to the relevant consumer forum under the Consumer Protection Act, 1986, a civil action for damages, a criminal petition under the Indian Penal Code, 1860, or file a complaint with the National Medical Commission (NMC). There is currently no specific law in India that governs online consultations provided by foreign medical practitioners.

WEARABLE DEVICES :

The use of portable devices has tremendously increased in India. Several portable devices are now available in India, such as heart rate monitors, monitoring blood oxygen levels, and other parameters including water consumption, weight, sleep, diet, etc. These devices allow patients to self-detect various physiological problems. changes in the body and also alert patients to problems. All medical devices are governed by the NMC Law, IMC Regulations, Medical Device Rules 2017, IT Law, and Privacy Rules. While there are no specific rules or regulations regarding portable devices, the above rules will also apply to portable devices. Under the current regulatory framework, these portable medical devices must be registered and approved by the Central Drugs Standard Control Organisation (CDSCO) in India.

[11]https://practiceguides.chambers.com/practice-guides/digital-healthcare-2021/india/trends-and-developments

For example, CDSCO very recently approved three portable medical devices in India, namely Smart Vital, Vital 3.0, and Vital EGC, from GOQii, a California-based fitness company that measures body temperature, pulse, ECG, tracks sleep, blood pressure, measurements are taken, exercise, etc.

ONLINE PHARMACIES:

New models of pharmacy have emerged focused on convenience, cost savings, and customer service - medications and home diagnostics are delivered to homes, often combined with counselling and support through a range of telehealth modalities. . As digital health products and solutions continue to develop, we may soon find that patients are routinely given medication as well as their digital companion as part of their treatment - transforming the patient experience of care and expanding the role of the patient. pharmacist as a drug expert to include digital health product curator, translator and coach. Specifically, pharmacists can play a role in matching patients with the most appropriate digital health products, helping patients configure products and train them in self-management, and access data for self-management. remote monitoring of patients to improve comprehensive medication management.

The pandemic has geared up the operation of online pharmacies in India, mainly for the online purchase and physical delivery of drugs to the patient's home. There has been a significant increase in the number of online pharmacies in India in recent years, more so during the pandemic. Although the manufacture and sale of medicines is regulated by the D&C Law, D&C Rules, Clinical Establishments (Registration and Regulation) Act 2010, NMC Act, and IMC regulations, there are currently no laws in place. India which specifically governs online pharmacies. The MoHFW issued a notification in August 2018

to amend the D&C rules to include online pharmacies within its jurisdiction (draft rules).

The draft rules include provisions relating to the sale of medicines by electronic pharmacies. In addition, the draft rules define the term "online pharmacy" as the business of distributing or selling, storing, exhibiting, or offering for sale drugs through a web portal or any other electronic means. The draft rules contain provisions for the registration and validity of electronic pharmacies, the registration conditions imposed on electronic pharmacies such as location, disclosure of information, the procedure of distribution and sale, etc. Electronic pharmacies in India currently require registration with CDSCO.

Further, online pharmacies will also need to adhere to confidentiality rules with respect to the collection, processing, and processing of a patient's sensitive personal information, including financial information, bank details, physical health data, physiological and mental, sexual orientation, medical records and history, and biometric information.[12]

ONLINE AGGREGATORS FOR HEALTH SERVICES

There are several new online platforms in India that allow users to search for doctors of different specialties in a particular region. These platforms also allow users to make online appointments with doctors and provide opinions and notes to these doctors for their services and advice. Currently, there is no specific law in India that regulates online health aggregation platforms. However, the MoHFW issued an instruction in January 2021 to all state governments to regulate e-health aggregation platforms. Over this , within the existing

[12]https://practiceguides.chambers.com/practice-guides/digital-healthcare-2021/india/trends-and-developments

regulatory framework, these online health aggregation platforms will have to register with CDSCO in the same way as online pharmacies.

The growing number of technologies collecting health data is raising concerns about data protection and patient privacy. Personal information relating to a person's health is classified as sensitive personal information under the rules of confidentiality. The confidentiality rules set out mandatory data confidentiality principles to be followed by legal persons who collect, process and process sensitive personal information. India does not currently have a comprehensive data protection law. The Indian government has released the Personal Data Protection Bill,2019 (PDP Bill), which is intended to become a comprehensive data protection law in the country.

There is not yet a specific law in India to regulate digital health tools and digital health data. However, the government has taken several new initiatives to address digital health privacy concerns in India as explained below.

ROLE OF TELEHEALTH IN MEDICAL TOURISM

Telehealth works on the quality, effectiveness and patient service in medical tourism industry applications by better coordination of care between suppliers in patients' home and other nations, improved preoperative and postoperative care, and advancing patient and relative travel. There are a number of preoperative telehealth applications.

Anaesthesiologists can perform tele-discussions, including remote physical appraisal of the cardiovascular and respiratory frameworks, including the aviation route. Postoperative consideration can likewise be given by means of telehealth after patients get back with virtual subsequent visits. Wound healing additionally can be assessed from a distance.

Telehealth would permit specialists to coordinate follow-up care with patients' neighbourhood essential care specialists and trained professionals. Improvements in remote checking innovation make it workable for postoperative home observing, conceivably relieving the danger of hospitalisation or decreasing the length of emergency clinic stays in the quick postsurgical period.

Finally, telehealth offers the possibility to improve customer service provided to meet the medical tourists. For instance, preoperative videoconferencing would permit patients, relatives, specialists and other key individuals from surgical staff to for all intents and purposes meet up close and personal.

Essentially, concerned relatives who didn't go with the patient could keep in contact with the patient or travelling relatives and get briefings or updates from the specialist or other key staff. This degree of connectedness could likewise be utilised to further develop congruence of care, by keeping the patient's care proved in their nation of origin required all through the perioperative period.

CHALLENGES

Although telehealth offers a huge platform in improving medical tourism, it equally poses several challenges. Legal and regulatory factors perplex the telehealth scene. In the United States, a telehealth doctor is viewed as practically shipped to the patient's state. Accordingly, doctors are needed to have a clinical permit in each state where their patients live. Additionally, the Joint Commission necessitates that the counselling doctor be credentialed at the office where the patient is located.

Protection and security issues should likewise be considered . For instance, the Health Insurance Portability and Accountability Act (HIPAA) applies to telehealth in the U.S. In any case, such risks can be avoided through appropriate

patient assent/approval. Also, specialised means are accessible to guarantee privacy , including virtual private organisation associations, document encryption and encoded videoconferencing.

In spite of the fact that there are a few lawful, administrative, specialised, and hierarchical hindrances to telehealth, they are surmountable. Telehealth will assume a huge part in the continued expansion and improvement of medical tourism.

EVOLUTION OF HEALTHCARE REGULATION IN INDIA

The Indian government has notified the Digital HealthCare Information Security Bill, 2018 (the DISHA Bill), to protect the digital health data of its citizens. The DISHA bill defines the term "digital health data" as an electronic record of information relating to the health of an individual. The government proposed the DISHA bill in 2018 to standardise and regulate the processes related to the collection, storage, transmission, and use of digital health data, and to ensure the reliability, confidentiality of data, digital health data privacy, and security. However, India is yet to pass legislation to regulate and govern digital health tools in India.

As a temporary measure, the Indian government released the GPT in March 2020, which contains norms and standards for licensed physicians to consult patients by telemedicine. The GPT regulates all channels of patient communication that operate information technology platforms, including voice, audio, text, and digital data exchange.

The Indian government also released a Health Data Management Policy in October 2020 to impose data privacy protection standards in India. Both the

DISHA Bill and the Health Data Management Policy are based on the data privacy principles set out in the PDP Bill.

TECHNOLOGY IN HEALTHCARE SECTOR ACCELERATED DURING COVID-19 PANDEMIC

The past year has been one of the most difficult years for the Indian healthcare industry and economy, amid the COVID-19 pandemic. Sadly, India's healthcare industry and frontline workers continue to face many challenges with the second wave of COVID-19, which hit India around the last week of March 2021.However, on the bright side in the healthcare sector, the pandemic has led to an unprecedented increase in the adoption and use of digital health technologies in India.

Digital healthcare is rapidly evolving during the Covid-19 Telemedicine is effectively helping in containing the spread of Covid-19. Video conferencing, virtual platforms, and self-regulating monitors are being used worldwide in order to control the spread of the contagious virus. The government of India (GOI) launched the National Digital Health Mission to digitise medical services and records all over the nation, and allowed telemedicine and e-drug store stages to offer consultations to avoid crowds at the hospitals. As on date, due to the unprecedented Covid-19 pandemic, individuals frantically need convenient medical care administrations at reasonable expenses, and technological innovation is assuming a key part in all spaces including supply chain management , patient consultation, online discussions, buying and conveyance of medicines.

This is the best opportunity to use technological advances to essentially work on the health sector all over the world. The interaction among health care and

technology works on the quality of medical care services with expanded access and reasonable expenses. It is intriguing to note that new companies are likewise thinking of developing advances to help the medical care area. The web-based medical services conferences saw a 500 percent development during the Covid-19 pandemic.

CONCLUSION AND SUGGESTIONS

Telemedicine is an astonishing innovation and keeps on holding the promise of being genuinely ground-breaking as far as medical services are delivered to everybody's advantage. As the populace keeps on developing at a rate quicker than the concomitant development in the quantity of accessible qualified clinicians and offices (institutional beds, examination research facilities, day-care focuses, and so forth), this innovation should be ideally saddled to guarantee that everyone who need care are taken into account essentially at acceptable levels, if not the most ideal.

Until today, many private sector companies have avoided making huge investments in telemedicine, because of the absence of a clear legislations approach and enactment. While a bunch of rules is accessible, it is neither exhaustive nor restricting. There is no normalised organisation to qualify patient–doctor association or to look for patient assent for protection and privacy. Further, there is no responsibility structure to handle medico-legal negligence matters or malpractice liabilities. The most pressing need is a reasonable strategy and enactment for delivery and reimbursements of services, like virtual discussions, computerised remedies and virtual ICU management.

Artificial intelligence can without a doubt carry new efficiencies and quality to medical services outcomes in India. Notwithstanding, gaps and difficulties in

the medical services area reflect profound issues around deficient financing, weak regulation, inadequate medical care framework, and profoundly implanted socio-cultural practises.

Today, doctors have plenty of information about their patients. With AI, this information can be utilised to upgrade medical services, doctor patient connections, therapies, and examination. Likewise, with AI, specialists and medical attendants can lessen manual work and focus more on their patients by furnishing them with more accurate service. If we add Machine Learning and Natural Language Processing (NLP) to AI, it can genuinely do wonders for health care systems all over the world.

The primary justification for ensuring individual security and privacy is to ensure the interests of people. Conversely, the essential legitimization for collecting personal health data for keeping a track on the medical records and help in health research which is a benefit for the society. In any case, it is vital to stress that privacy additionally has esteem at the societal level since it grants complex exercises, including research and general health activities , to be carried out in manners that ensure individuals' dignity. Technical safeguards like firewalls and secure transmission modes for communication such as virtual private networks (VPN) and secure socket layers (SSL) etc and other encryption techniques can be used to protect and preserve the patient's medical health data.

The changing environment of each area from desk work to electronic records is at an exceptionally high speed and this change from paper to everything on the web needs assurance of information and a total watch. In India, just the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 is available while many Acts are yet to be made or upheld. In any case, there are such countless holes in the approaches made or in-production, in light of the fact that on one side it gives the right to security and on the other, it says

that anybody can profit from the data or look to get to the records under the Right to Information Act, 2005.

The State, for an effective framework, needs to assume a functioning part while making laws in regards to security and privacy in medical care and it ought to likewise empower the support between the various foundations, both in the private and public area. The joint endeavours of these sectors or numerous multiple needs to ensure one of a solid and incredible central system in the country on which the Right to Privacy and Confidentiality in medical care can be effectively built.