Big Data in Electronic Health System and its Challenges

Aranya Nath,

School of Law, GITAM University, Vizag, subhamitanath002@gmail.com 0000-0002-1705-2793

Kodukula Venkata Lakshmi Priyadarshini,

School of Law, GITAM University, Vizag, kodukulapriyadarsini17@gmail.com 0000-0002-7566-6662

Poushali Das,

Junior associate at Minus dispute legal Strategists daspoushali.1997@gmail.com 0000-0002-4976-842X

Antara Paral,

BBA LLB IFIM Law School Bangalore, antaraparal2018@gmail.com 0000-0002-1680-8982

Gautami Chakravarty,

BA LLB IPR KIIT School of Law Bhubaneswar gautamichakravarty21@gmail.com 0000-0003-4579-6754

Naisargika Mishra,

BA LLB Business Law KIIT School of Law Bhubaneswar naisargikamishra@gmail.com 0000-0003-4414-4252

Article Info

Page Number: 6679 - 6801

Publication Issue:

Vol 71 No. 4 (2022)

Abstract

During the 18th Century, where no Digitalization was there in any sector, the paper-pen-based data method, also referred to as the traditional method, was followed. From that perennial moment until today, science has flourished into various revolutions in every sector. The health sector is one of the most significant areas with a considerable level of intervention. Health care, which is inextricably related to life in general, has exhibited increasing reliance on advancing Technology, which has taken the lead in the name of a Digital Revolution in the health sector. The authors, through this chapter, seek to discuss the same and its link with Information Technology and Data Privacy guidelines in a descriptive manner. The Study will be started by the overview of the Technology used in the health care industry to the present techniques prominently used by doctors and physicians worldwide while we are in a pandemic situation. It would help the readers understand the revolution since its known significant inception. As the Covid-19 pandemic hit, the medical field triggered innovation. On the other hand, after the advent of Technology in the Healthcare sector, most of the Healthcare Data has been digitized, which refers to Electronic Health Records in the Healthcare Information system; it will discuss IPR management and Data Privacy Laws in this scenario.

Keywords: Artificial Intelligence, Big Data, ethical, legal challenges, Healthcare Data, Privacy Laws.

Article History
Article Received*: 25 March 2022*
Revised*: 30 April 2022*
Accepted*: 15 June 2022*
Publication*: 19 August 2022*

1 Introduction

The current scenario of the medical field has great importance on the public at large. Nowadays, in the advancement of information technology, Healthcare has been shifted to a new advanced form from clinics/hospitals to homes.[1] Doctors address health-related issues earlier, but many shortcomings often occur due to a lack of proper care or diagnosis. With the help of technology, doctors have introduced various techniques to provide better treatment facilities to the patients to provide smart health care. [2] Smart health care is not a simple thing; it requires various models for improvisation. Our Indian Government in the "Make in India" project [3] stated that it would appropriately address all kinds of shortcomings with the latest form of technology in health care. It also provides a comprehensive analysis of the usefulness of the technologies.

As we're well aware, the current medical services field is going through critical changes at the turn of the decade. Many of these depend on ongoing innovative advances and mirror an expanding pattern towards customized medication.[4]

In the era of Digitalization, Big Data proved to be one of the advanced technologies in medicine. It brought great hope in medical research in the personalized treatment of medication.[5]

The invention of various kinds of novel medications reduces the cost of the patient by providing the best treatment facilities. The most prominent features are that it helps keep ample storage of massive data that consists of patients' health records and other sensitive information.

The Digital Health Revolution commenced after the post Pandemic scenario to maintain the social distance in hospitals. In May 2018 World Health Organization passed the guidelines of "Recommendations on Digital Intervention for Health System Strengthening,"[6] which aims at providing m-health and Telemedicine, which has become effective after the scientific research development.[7]

To prevent the spreading of Covid-19, Smart hospitals are enabled. The traditional method of keeping handwritten medical records transforms into Electronic Medical records (EMR),[8] which aims to utilize information by collecting a large volume of data. Therefore, it can produce alarm signals and communicate the patient health information, particularly to create a biomedical system and a health monitoring system in real-time, has gained traction.[4]

Big Data in Healthcare where every possible work gets sorted out by utilizing the efficiency of a massive compilation of data stored for the better improvement of the patient in service delivery. We all know that the medical profession's ideals are based on mutual respect and confidentiality. It recognizes as the foundation of the medical profession until the Greek philosophy era. Therefore, Telehealth [9] becomes a reality in India after the Covid-19 pandemic hits. Big Data plays an essential role during that time. It potentially saves a significant massive volume of data about the individuals treated with the COVID-19 virus to a comprehensive knowledge of the virus's nature. The information obtained will then be analyzed to establish upcoming precautionary measures. This technique is often used to store data from all categories of COVID-19 cases (infected, recovered, and expired). The data can be leveraged to detect significant cases and allocate services to maximize health care security.

While implementing Big Data in the healthcare sector there’s several advantages and prospects, it also introduces significant shortcomings. The most prominent issue arises from the security and privacy issue due to the intensification and advancement of technologies for collecting Digital Health Records(DHD). It is possible that the digital health data (hereafter 'DHD'), including patients' personal health information, is exposed to significant privacy-related threats. Whereas the usage of DHD appears to be viable enough to change India's healthcare completely, user behavior monitoring is on the cusp of being implemented without the prior approval of patients. The hazardous convergence of the right to privacy with the need for Healthcare necessitates the security of individual health records. A patient's personal health information is recorded and archived digitally at the point of treating patient, from his initial admittance at the hospital to his final diagnostic procedures. The database is available and accessible to all healthcare practitioners responsible for the patient; however, the scope and nature of data collecting are highly unusual. Not to acknowledge the risks when this information blends with source information, such as pharmaceutical companies, leading to deceitful sales promotion, privacy violations, exclusionary segmentation, and re-selling sensitive data instead of commercial internet transactions. The main issue is safeguarding privacy with the Data collection in Big Data Technology.[10] As per National Health Policy 2017[11] Digital Information Security in Healthcare Act (DISHA), Bill [12] was primarily set up to look into the issues related to the privacy of medical health records. Is there no proper legislation that has evolved to date?

As we all know, Big Data Technology has evolved after the Covid-19 pandemic hits in India. However, under Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 (in the future referred to as IMC Regulation) go amended recently were the guidelines for Telemedicine and M-health concepts given better clarity.[12]

As a result, the readers will be able to comprehend the concept throughout this entire research of various technologies used in Healthcare and also the Socio-legal aspects of technology along with the jurisprudence of the present Healthcare and Big data in world comprehensive as per OECD guidelines[13] along with the rights of the individuals in case of privacy and confidentiality related issues.[13]

1.1 Literature Review

R.C. Goyal, Handbook of Hospital Personal Management, Prentice Hall of India, New Delhi, (1994) – The methods and measures of planning, organizing, staffing, directing, and controlling a hospital and its administration were explored in depth in this study. The author emphasized the use of scientific methodologies to improve the hospital's entire services, management, and thus the patients.

The application of Section 304A of the Indian Penal Code to doctors and the importance of patient consent before operation were discovered through this research. The discussion on Medical Negligence or Deficiency in Service that took place in this book paved the way for a greater understanding of patient rights and related issues.

M. Chalapathi Rao, A. Kiran Kumar, Challenges arise of Privacy Preserving Big Data Mining Techniques, International Research Journal of Engineering and Technology, Vol.4(5), 234-236 (2017) – Big data is being generated from various sources-transactions, social media, sensors, digital images, videos, audios and for domains including healthcare etc. this data is known as big data. The author opined that useful data can be extracted from this big data with the help of data mining techniques the massive volume of big data sets is too complicated to be managed and processed by conventional relational databases the term "Big Data" was coined to address this massive volume of data storage and processing.

Dr. Fatma Mohammed Abdullah, Privacy, Security and Legal Challenges in Big Data, International Journal of Civil Engineering and Technology, Vol. 9(13), 1682– 1690 (2018) – It is known very well that business all over the world are using big data to improve their techniques and process and make best decisions. Big data has become an irreplaceable a part of every financial system, organization, business strength what is more character. traditional database structures aren't always capable of capture, store and analyses this huge quantity of data. security and privacy issues are intension via velocity, volume, and variety of big data, which includes big-scale cloud infrastructures, range of statistics assets and formats, and high quantity inter-cloud migration. Therefore, the author stressed in this study that the conventional safety mechanisms, which are tailored to securing small-scale static data, are inadequate. With a rapid growth of data, whether the traditional security and data protection still adequate to be adopted into big data architecture and environment is questionable. This study discussed the security and privacy issues in Big Data and investigates legal challenges in Big Data processing. The author has addressed how big data is an appropriate method of study it may be a part of for a long time. However, legal issues with large volumes of data imply that processing and interpreting big data will creep over the next few years. Legal issues linked with broad knowledge correlate to obtaining and using data. It is one of the first legal issues that clash with vast information.

2. Evolution of smart healthcare and big data

From the age of the ancient beings to the present phase of the hustling humans, the perennial affair between life and technology has stood against the stubbornness of time. Be it the invention of wheels, or that of the flying machine to that of the artificial brains, technology has time and again proved to be inevitably and increasingly necessary for the sustenance as well as progress of life. Having said that, one of the most prominent sectors which have witnessed a high level of intervention is the health sector. Very intricately linked to life in general, health-care has been showing growing dependence upon evolving technology, which has taken the name of a Digital Revolution in the health sector. The authors, through this chapter. The chapter begins with the authors tracing the past trends of technology used in the health care industry to the present techniques which are being prominently used by doctors and physicians worldwide while we are in a pandemic situation. This would help the readers to under the 'revolution' since its known significant inception. Additionally, the authors also contemplate the causes that are believed to have triggered such an evolution and its subsequent entry into the medical field. As evidently noticed, COVID – 19 situations have acted as a catalyst for digital innovation in healthcare. The researchers suggest the concept of innovation which leads to faster innovation, especially in terms of rapidly ratcheting up e-health competencies. The chapter begins with the authors tracing the newest form of technology prominently used by doctors and physicians worldwide. This would help the readers understand the current emerging technology in smart health. In addition to it, the authors will contemplate the pros and cons of the recent emerging technology, which has significant inception.

3. Concept of Healthcare and Smart Healthcare

1.2 Healthcare

When we talk about the term "health care" the first thing that comes into the mind of the reader is the USSR declaration for healthcare. The term" healthcare" is defined as the efforts given by the medical practitioners to maintain physical/ emotional & mental growth of a well-being. Earlier the techniques are not well equipped for the treatment whereas in the 21st-century medical technologies and treatment procedures are well advanced. Thus, the concept of smart healthcare comes into the picture. According to Blue stream, Smart healthcare means services rendered to the patient through some wearable devices and with the help of advanced medical techniques or diagnostic tools. The healthcare sector typically benefits greatly from the use of information technology, specifically IOT & Big Data. As of now, this study throws a light regarding the advancement of the latest techniques so it is of utmost necessary to look into the legal protection of those technologies and that asset can be managed. The transformation from healthcare to smart healthcare demonstrates itself in the following ways: changes in methodological approaches (from illnesses to patient-centered care), changes in the implementation of the information development (from diagnostic digitization to regional medical Digitalization), alters in ongoing treatment (shifting attention from illness treatments to preventative healthcare).[14]

1.3 Smart Healthcare

As we've already introduced the concept of "Healthcare"[15] and "Smart Healthcare" therefore it is of utmost necessary will go into the origins of smart health care in detail. The concept of "Telemedicine "has been considered as a natural evolution of smart health care. The term Telemedicine was coined in the 1970s.The Greek word "tele" means "distance," and "mederi" means heal.[16] Medical science is getting advanced day–by–day with the latest technique that utilizes sensors for information perception Transmit IOT information and store information through cloud storage.[17] Now when we say some presentation or any form of technology is a 'smart' way of presentation it reflects how the whole system has been properly summarized adequately so here in the healthcare industries smart healthcare refers to proper management of hospital systems in one platform via virtual mode. Medical data are large so to handle all the matter efficiently cloud platform is required. When the patient gets registered, they can pay the bills of the reports online. Moreover, technology changes society along with fueling the network connecting industries which creates enormous changes with the new generation of technology.

4 Legal challenges of big data in health care

There is an ever connection of highly diversified encrypted data generating innovations in medical, biomedical, and healthcare fields. The growing availability of data in a central place used in need by any entity, ranging from pharmaceuticals to health insurance companies to hospitals, has also primarily put health professionals with all its sub-sectors in the face of a flood of big data before seen. Information advances in the disciplines of medicine and healthcare. The increasing metadata in a centralized place for use by any entity, ranging from pharmaceuticals to healthcare insurance companies to hospitals, has essentially opened health professionals and their sub-sectors to a deluge of big data never seen before.[18] While this data is being acclaimed for improving patient care, acquiring valuable knowledge, and lowering costs, confidentiality issues are so formidable that the healthcare sector will not effectively manage its current resources. On either side, regulating and harnessing the quantitative potential of big data is pivotal to the survival of all healthcare providers. Big data has also significantly altered the way companies gain, evaluate, and use information across all industries. Among the most emerging field in which big data can contribute meaningfully is healthcare. We evaluated the state-of-the-art security concerns in big data, evaluated what privacy issues occur inside the case of massive healthcare data, and presented approaches to handle individuals in this study as applicable to a health sector. We focused on recently proposed confidentiality and encrypted procedures, their benefits and limitations, and future study possibilities.[19]

Our latest scenario of digitization of healthcare procedures & transitioning to digitized patient information has culminated in a radical transformation in the healthcare industry. The amount of patient research that's also technologically available will be significantly expanded in terms of depth, variability, and timeliness, culminating in what has been known as big data. Big data is committed to having a full range of potential experiences and to use cases, such as the following specific examples: Big data, driven by legal responsibilities or the chance to improve healthcare, saving lives, and improve efficiency, has the prospect of delivering an infinite number of possibilities and use scenarios, including considering disorders impacting several significant organs, patient care, health insurance, prevention strategies, population health management, adverse reaction monitoring, and therapeutic personalization are all available.[20]

While implementing big data technology in the healthcare sector has several incentives and prospects, it also introduces significant limitations and problems. Indeed, due to multiple emerging health issues, concerns about sensitive information privacy are increasing from year to year involving areas such as clinician mobility and networking technologies, health transfer of information, cloud computing, and so on. Furthermore, healthcare providers realized that a proactive, bottom-up, innovation methodology was effective. for identifying safety and privacy[21] needs are insufficient to safeguard the business and its patients.[22] Every healthcare business must adopt a proactive, preventative attitude and actions to prevent sensitive data thefts and other data breaches, focusing on future security and privacy concerns.

4.1 Synopsis of Indian Medical Practices

There are two categories of healthcare technology in India: public and private. The law governs public healthcare, which is available to everyone. The industry covers super-specialty hospitals which are outfitted in drugs and equipment and are often located in metro- cities. Moreover, district and taluk hospitals provide healthcare to the population. There are low-cost primary healthcare facilities and the rural hospital offered that assist an individual with reasonable treatment.[23] The private sector is considered equivalent and primarily used by the upper- middle and upper-class populations. The total cost of healthcare services in the private sector is costlier than healthcare services in the public sector.[24]

4.2 Health in India: Policy Reform Study Focused: National institute Aayog Report about India's Health Industry

The Indian government is proactive in the health sector and encourages global investment. The Indian government intends to increase public health care spending from 1.1 percent to 2.5 percent of GDP over the next four years, according to "NITI Aayog." The conclusion implies that India is committed to providing progressive healthcare to all citizens. The Indian government invests 1.13 percent of its current GDP in asset value. According to the NITI Aayog research, India's healthcare system is inadequate and fragmented due to cultural and religious diversity or bad policy implementation. A solid financial basis and reform efforts are required to transform the failing healthcare business. The Indian economy is expanding. In another few years, India had maintained costs under control, increased GDP, and encouraged states to become strategy. Indians' health has improved over the previous decade due to a positive financial foundation. Health records, patient medical analyses, skilled and professional health advice provided by machines, and smart technology data analysis are all employed in India. Because of qualitative advances in India's health and healthcare sectors, the "Make in India" policy encouraged investors to spend more in the healthcare industry.

Upgrading the healthcare system can reduce mortality and poverty rates while accelerating economic growth. Developing sensitive, intelligent, and automated health systems can assist Indians in improving their healthcare and lowering their morbidity and poverty rates. Applying AI and machine learning algorithms to digitized Indian healthcare data can enable illness detection and advanced counseling of medical specialists. The standardization of medical records can help patients obtain information faster and boost the usability of healthcare records. The fundamental issue with India's healthcare industry is needless and non- uniform health sector fragmentation. The primary factors for India's healthcare systems' lack of performance include data fragmentation at any level and its granularity. Decentralization, distinguished by a plethora of institutions, entities (formal and informal rules), strategic planning, and institutional procedures and entitlement programs which do not synchronize harmoniously and are frequently subject to contradictory incentives, severely impedes continuity of care and portability benefits. Healthcare system fragmentation exists in other jurisdictions with consistent regulations and norms and the same set of responsibilities to access it. Uniform and reduced fragmentation of healthcare data and consumers are practical:

- Safeguard healthcare information protected from unauthorized parties.
- Have consistency in consolidated healthcare systems.

Indian healthcare laws are changing[25] and have become more monitored. Must address several current healthcare concerns to protect the networks outlined.

4.3 Concept of Healthcare Privacy

Patient privacy is an essential feature and jurisdiction of all governments globally, and then all nations have recognized that they must maintain people's privacy at all costs. Individuals have an inherent right to privacy. Some countries (particularly those in Europe and the United States) place a high value on privacy policies. Recent regulations such as HIPPA and GDPR provide consumers' confidence in their privacy issues and help them create trust. However, no uniform concept of privacy exists as of yet. Some meanings are perception-based and vary by country. The following are many meanings of privacy.No one shall be subjected to arbitrary invasions of privacy, family, home, or communications, or threats on the dignity and character. Everyone has the right to legal protection from such interference or assaults, says Article 12 of the Universal Declaration of Human Rights. Privacy is the right to be alone or free from disturbance or intrusion. The worldwide association of privacy experts defines information privacy as the right to have discretion about how individual sensitive data is produced and processed.Since healthcare data confidential patient information and other stakeholders, confidentiality is essential in the healthcare profession. As mentioned, initially, most healthcare professions have shifted operations shift from illnesses to diagnoses. People's records are kept based on their characteristics, personal and emotional behavior patterns, and location data. One of the best solutions for data evaluation is the central storage of digitized health data across structured computers. Because of its centralized monitoring and retrieval, it minimizes the utilization of duplicated or redundant data. The volume of health records is substantial, and the information in India is indeed unstructured. Furthermore, storage and transformation issues might lead to privacy and data breaches.

Privacy is not regarded as a severe issue in India. Data privacy in healthcare is exacerbated by ordinary carelessness, tradition, politics, budget constraints, a growing population, and technologies in India. With these considerations, data security needs come second in giving simple access to private information. Furthermore, healthcare confidentiality in India is influenced by the current culture. Having to disclose highly confidential health records is considered upon in many cultures. It results in errors inside the documented healthcare data and reduces the amount of therapy provided. Because of erroneous data collection, both outcomes and demographics of medicines administered do not correspond to the records.India is a democratic country with a considerable population, and adopting privacy concepts in India is difficult due to the lack of consistent infrastructure.The expense of implementing a security paradigm is significant, and it requires support from both the government and the people. Making the privacy model a success necessitates the efforts of experts in the disciplines of privacy and healthcare. Due to some financial concerns, an inefficient design that is not secure and protected from assaults may be developed.

According to recent reports, the Indian health ministry has suggested an information security law (personal data protection bill) that would give citizens total control over their data. People can view, distribute, or reject access to the server's records. On March 11, 2018, the Health Ministry recommended digital information security in the Healthcare Act. The group made the following recommendations and created a privacy framework:

- The law has to be adaptable to evolving technology.
- Law applies to both the public and private sectors.

- Organizations in charge of data should indeed be held accountable for data processing.
- Systematic and authentic consent is required.
- It must keep information analysis to a minimum.
- A robust legislative body should enforce an information security system.

The Indian healthcare information is quite varied and comes from various sources (public and private sector hospitals and health insurance). Because there are no guidelines governing health data authoring, any service provider can obtain confidential material and exploit it. The proposed law includes principles and technology features safeguarding the confidentiality of healthcare data.

5 Big Data Security issues in Healthcare

To enable effective and appropriate treatment, healthcare institutions collect, manage, and transfer massive volumes of data. Nonetheless, protecting sensitive data has been a difficult task for centuries. The healthcare market remains among the most vulnerable to publicly reported data breaches to worsen the situation. In essence, Cybercrimes could employ data mining processes and techniques that identify confidential material and distribute it to the public, culminating in a data breach.[26] Although deploying security precautions continues a challenging process, the consequences always rise as new technologies that overcome vulnerability analysis emerge. As a result, enterprises must adopt healthcare data protection systems that safeguard valuable systems while meeting healthcare regulatory requirements. People in charge of protecting sensitive patient information must use extreme caution to meet all regulatory data requirements. It's virtual a "no-choice" situation considering healthcare protection is not something that can be taken lightly with such freedom in implementing authentication and authorization. On the front end, it ensures that the overall has incorporated several approaches. Single sign-on, authentication systems, and patient registration are examples of how to enhance credibility amongst customers, technology, and information in the healthcare sector.[27] Most medical patients don't worry about their security when they go to the doctor; most want their data and health handled safely. Unfortunately, this is not always the case.[27]

5.1 Multi-factor Authentication

Passwords may be vulnerable for programmers, especially when new tactics that need media manipulation to leverage security software vulnerabilities, including password spray assaults and phishing.[28] It is where multidimensional authentication (MFA) approaches can help to give an extra layer of identity security. MFA requires users to provide a combination of variables — at least two — to validate their identity and get access to a computer or device. The factors are divided into three categories: who you are (like a biometric fingerprint), what you have (a portable phone), and what you know (a username and password).[29] According to Wright, a typical two-factor authentication mix would include the user's login and password and the token number from the user's smartphone.

Biometric sensors that recognize distinctive physical features, such as biometric authentication or retina scans, are also used in some technologies. Furthermore, cyberattacks are still among the top concern challenges for healthcare professionals. According to a HIMSS study earlier this year, transitioning away from passwords is even more critical. MFA dramatically improves security, so there is such a strong drive to guarantee that all high-level accounts are not accessible without some MFA.[30] Furthermore, MFA can serve as a portal for password-free authentication.

Microsoft has already achieved a pseudo-password-free state for its clients by internally installing several of its MFA solutions.

5.2 Final encryption

There are two main concerns confronting healthcare cybersecurity, none of which can be handled only by increased efficiency. The primary issue is that healthcare is an essential factor in our society.[31] If you want to cause devastation, maybe the most significant way to start is to destabilize a country's healthcare system. Electronic Health Records also are hugely lucrative health records in electronic medium. The second challenge is that security is a shared responsibility, even within a single facility.[32] If a resource is often distributed, each party's objective is to attain as much benefit as feasible while spending such little expense as possible.[33] It is referred to as the commons tragedy. End-to-end authentication is based on Public Key Infrastructure (PKI). PKI provides electronic certificates to authenticate people, systems, and devices, eliminating the necessity for credentials, security protocols, and other time-consuming user-initiated variables redistributes authentication and enables it to occur across several platforms. End-to-end identification may not be accomplished in the healthcare industry unless device manufacturers, hospitals, insurance companies, software providers, and security vendors understand and accept their joint responsibility. Because of the rising number of breaches in healthcare, cybercrime is becoming a significant area of concern for people working in the industry. This suffering prompts some people to act differently and put more safeguards.

6 Privacy and Data Protection Laws

In access to the increasing complexity of federal data protection laws, healthcare providers must manage and secure personal information and address their risks and legal duties regarding personal processing data. Distinct nations have various data privacy regulations and legislation. The following table lists data protection regulations and laws in some of the countries and critical elements.

Country	**Laws**	**SalientFeatures**
United States	HIPAAAct Patient Safety andQualityImprovement Act(PSQIA)HITECH Act	• Minimumstandardsforelectronichealthcareinteractions arerequired. • Individuals aged 12 to 18 are entitled to therightto privacy. • It must not reveal the patient's Proper SafetyPackage before providing information aboutdelivering health care to anybody, includingparents, • A signed disclosure from the impacted isrequired. • Protectpeople'sfundamentalrightsandfreedoms,itshould notbe disclosed. • Individualswhobreachtheprivacyrequirementsfacelegal penalties. • Protectthesafetyandconfidentialityofelectronichealth records.
European Union	Data Protection Directive	• Safeguard specifically their privacy rights regarding personal data. regarding personal data processing.[34]
Canada	Personal information protection and electronic protection	• Individuals[35] have the right to know why their sensitive data is being collected or used, and entities are obliged to safeguard this information in a legal and safe environment.
UK	Data Protection Act (DPA)	• Humans can control the flow of information about themselves. It should not transfer personal data to a country or territory outside the European Economic Area unless that country or area guarantees adequate protec-

		tion for people's rights and freedoms.
India	Information Technology Act 2000	• Use acceptable protective measures while handling sensitive personal information. Compensation provides to individuals who have suffered unlawful loss or gain. Provides imprisonment and fines for anybody who causes unjust damage or increase by releasing another person's confidential info while performing services under a legitimate contract.

Healthcare providers are also entirely consistent in their framework for analyzing security risks. According to the survey, the most significant barriers to cybersecurity rehabilitation and mitigation are a lack of qualified Cyber professionals and a lack of financial resources. Organizations may deter attacks by implementing effective filters that prevent them from occurring in the first place. Big data security is seen as a significant obstacle in this industry for scientists. Big data has limitless potential in advancing health research, knowledge discovery, clinical treatment, and personal health management. However, various constraints and problems, including technological challenges, privacy and security concerns, and a lack of competent people, restrict its viability in the healthcare area. The security and privacy of big data are being considered.

1 Human rights issues of Big Data in Healthcare Indian Scenario

An ethics interest in human rights considers and assesses law in terms of underlying moral implications. Some human rights implications of data-driven medical services address here, emphasizing the rights of people who live with disabilities and are thought to be at an increased risk of developing a disability in the future. First, in the digital technology revolution's history, fundamental principle issues such as equity, equality, sustainability, and security arose. Therefore, big Data's qualities and features are studied to understand new value issues fully. Using these evaluation measures contends that big data necessitates two types of human rights evaluations.

The first is a re-evaluation of existing human rights in the digital domain, namely through the right to equality and the right to employment. The second step is to conceive new digital rights, including an individual's right to privacy against stereotype exploitation. Access to high-quality data at a fair price can assist governments in fulfilling the well-established right to health under international human rights law. People have also gained more control over their health due to the data revolution and the ability to monitor their governments adherence to human rights accords such as the Convention on the Rights of Persons with Disabilities (CRPD). However, big data might unwittingly encourage prejudice and privacy abuses. In principle, governments should safeguard the confidentiality of people's health data. It isn't easy to prevent data miners from using re-identification techniques to link unencrypted health information with non-medical open data.

With the introduction of Covid-19, Telemedicine innovations have been lauded as an effective measure to reduce deficiencies in the delivery of high-quality health care and a crucial component in achieving the SDGs. Technology, on either hand, poses privacy and confidentiality risks, leading to discrimination and oppression, resulting in violations of the rights to health and security. Without adequate planning and safeguards, digital health innovations have the power to exacerbate access to care by extending the technological barrier, which separates those who can and cannot employ such medicines.

Value systems are underlying the development of modern human rights, which would be inextricably linked to the development of liberalism as an ideology. The development of the 'Rights of Man' emerged from a historical basis that prioritized people's financial, political, and military use to unify nations. Later in the twentieth century, liberals joined forces with capitalist ideology to resolve the growing tension between distribution (ethical) and production (economic progress) by developing the conception of "human rights." Human rights have developed through four decades of freedoms since then: civic engagement rights, socio-economic rights, and the power to self-determine. As doctors and other healthcare professionals are expected to keep extensive records of patients' medical history, illnesses, treatments, and progression toward medicine, the healthcare sector has historically generated substantial volumes of data. The type & volume of patient-related information increased dramatically when medical record-keeping migrated from hard-copy files to digitalized records. Administrative records, such as insurance and payment records, can potentially provide health-related information. Individuals increasingly routinely reveal their health-related data, whether through work-based "wellness initiatives," health information sharing websites, or other social media. Twitter has even become a source of public health statistics.

The methods for storing, collecting, and interpreting this data have likewise expanded quickly, opening up vast prospects for professional researchers and scientists. Thus, in the age of "big data," academics must handle large, diverse, but incredibly quickly data sets increasingly accessible to the general public. Human rights experts and monitoring entities acknowledge that "big data" may have good and bad consequences for human rights. The problem is to discover strategies to reduce destructive impacts while not unreasonably reducing the potential for beneficial outcomes. Although much of human rights experts' emphasis has been focused on the right to privacy, big data has implications for many other human rights, including the right to health and the right to life.

Firstly, it discusses about the How big data could advance our right to health, which acknowledges in international law and many national constitutions. Big data has the potential to enhance medical research, improve patient outcomes, make healthcare more accessible, and users must be able to take more responsibility for their health.

Big data may also help individuals exploring disability and health, as well as make it simpler for campaigners to track their governments' adherence to human rights accords. Second, big data pose enormous dangers to privacy and equality rights. Employers, financial institutions, and insurance firms, for example, have a solid motive for discriminate not just against people who've had present impairments but also against those who are thought to be at risk of developing impairments in the future. Individuals frequently believe that their health-related data would be kept private or disguised before being public. Data breaches are, unfortunately, all too prevalent.

In early 2020, governments attempted to constrain mobility in response to the situation of stopping the spread of a little-known and fast-moving virus, includes Lockdowns, travel restrictions, and prohibitions on main festivals. In the absence of therapeutic interventions, countries strive to increase social distance, detect and isolate individuals infected with the SARS-CoV-2 viruses that cause COVID-19 illness, and close quarantine contact information of those sick and individuals having arrived from areas with high levels of infection.

Several countries have looked to Digitalization implementation and advancement to respond to COVID-19. New technologies such as infrared thermal screen cameras and wearables have enhanced fundamental e-health solutions, including digital COVID-19 data panels and smartphone applications for illness detection and planning activities.

7 Issues in Right to Digital Health Technologies

Lack of access (the "digital gap") or commercialization in healthcare are two possible human rights issues that can arise from using digital technology for health. Data breach, biases, and functionality creep were three potential problems associated with digital health technology that might be tied to privatized and public health systems. Understanding each is essential for limiting the adverse effects of digital health technology.

7.1 Violation of Information

A data breach defines as any cyberattacks those results in the "accidental or illegal destruction, loss, modification, unauthorized disclosure, or availability of personal data."[36] Data breaches are widespread in the healthcare market.[37] It influences many reasons, including viruses and cyberattacks and the unintentional or intentional exposure of protected health information by healthcare staff. Individuals' privacy rights are being infringed, and trust in the healthcare system is eroding. As technology advances and healthcare systems get more complex, data theft becomes more likely. Health systems must invest in information security and data protection to detect possible risks; yet, not all health systems have the resources.

7.2 Discriminatory Practices and Biases

Due to computational inefficiencies in AI and other automation processes, differentiated treatment is observed on numerous times. This phenomenon, for example, might exacerbate prejudice in criminal law proceedings and anticipatory enforcement, foster discriminatory hiring selections, and generate discriminatory online marketing activities. According to research on advanced technology in health care, analytics need not yield consistently precise predictions of survival rates irrespective of race, gender, or socioeconomic class. It raised questions that AI will further entrench discriminatory practices towards humans on these grounds. The UN Special Rapporteur on Contemporary Forms of Racism is conducting research on new communication technologies, non-discrimination, and minority rights to tackle such concerns. Moreover, some computerized selection avoids present anti-discrimination legislation, culminating in unjust distinction that is technically lawful but contradicts the purpose of achieving the right to health for everyone.

7.3 Functionality Encroachment

When data is gathered for one reason (for example, personal information provided as part of a medical screening) is used for another, this is associated with active invasion (such as checking immigration status). Concerns about function invasion cover a wide range of digital health devices. Nonetheless, they are essential in fingerprinting, where fingerprint data is collected for healthcare technology purposes, for example, might be utilized for forensics or criminal proceedings.[38] Functionality creep could also result in data thefts when, for instance, devices like fitness trackers expose information that can use to identify people's residences,[39] are frequent. Collaborations between the administration and commercial businesses, notably large technology firms, have also prompted concerns about the possibility of functionality encroachment to know the advantages of espionage or commercial objectives.[40]

8 International Perspectives on Ethics and Human Rights

So far, discussions about possible risks from digital health technology have concentrated on establishing ethical principles and norms. There has also been debate over implementing legally enforceable IHL obligations. [41] Although there may be some conceptual overlap in concepts, ethically and individual rights should be regarded as independent but complementing frameworks for protecting people and encouraging accountability for efficient, just, and people-centered digital health technology.

8.1 Strategies for Ethical Values

Several entities, along with the Institute of Electrical and Electronics Engineers, the Economic Forum, and the European Commission's High-Level Expert Group on Artificial Intelligence, have produced ethics and digital technology information.[42] The United Nations' Chief Executive Board is also working on suggestions on the ethics of artificial intelligence. Most ethical frameworks highlight that digital health devices should "cause no harm," They involve a responsibility to be aware of and avoid any potential downsides. In addition to reducing negative impacts, technology should enhance advantages for users.

Theoretical approaches likewise encourage involvement and participation, asking creators and public officials to assure that end users are actively implicated in the formation of digital technologies. Furthermore, the development, adoption, and deployment of digital health solutions should take place in open, discoverer environment that allows for public discussion, monitoring, and consultation, as well as ensuring computational openness, for example. Ethical frameworks also underline that digital health technology should not allow discrimination against humans, whether intentional or unintentional. Furthermore, ethics emphasize the need of equality. It encourages people developing digital technology to take into account the requirements of vulnerable and disadvantaged populations such as women, children, racial and ethnic minorities, and migrants. It entails ensuring that everyone has access to appropriate non-digital alternative to Digitalization. Developing theoretical approaches of digitized medical technologies can be crucial for promoting rights and avoiding harms, and these frameworks are routinely employed to manage private actors, whether individuals or businesses. Ethical principles, on the other hand, can be hazy.

As a result, sanctions may be ineffectual. Adopting and implementing human rights norms and standards that codify core moral principles in law can increase the likelihood of enforcement and accountability considerably.

9 Frameworks for Regional Data Protection

The right to privacy is a fundamental right established through regional treaties. The African Union Convention on Cyber Security and Personal Data Protection, the Asia-Pacific Economic Cooperation Privacy Framework, the European Union's General Data Protection Regulation, Ibero-American Standards for Personal Data Protection, and the Council of Europe's Westernize Convention on the Prevention of Individuals concerning the Processing of Personal Data are examples of such agreements. Many of these frameworks focus on data privacy and surveillance, and they have built protections for data processing and the rights of persons whose data is gathered.

Including these regional frameworks, information should be collected and applied in a manner that:

It is legal, reasonable, and straightforward to personal data.Consistent with a useful purpose indicated by the subject and consented upon by personal information. Have individuals classified the basic standard required for the lawful reason? It is only kept for as long as is required for the specified, legitimate purpose. It guarantees optimized data reliability and completeness, and secure information.

Maintains data reliability and reliability of the informationFor data collection procedures and use, should seek explicit authorization. Such permission must grant voluntarily—an unequivocal yes to a request stated in clear and transparent terms. Additionally, institutions (states or businesses) that information must take precautions to maintain cybersecurity, including privacy protection or anonymization and personal data encryption. Such regional frameworks also include positive data on subjects' rights. These data subject rights include the following:

The right to be informed about what information is and is not collected;

- The right to access stored data;
- The right to correction;
- The right to restriction of processing;
- The right to be notified of rectification,
- Erasure, or restriction of processing;
- The right to data portability;
- The right to object; and
- Rights related to decision- and profiling.

10 Conclusion

The analysis of the entire research conducted on Big Data in healthcare indicates the innovative method in Digitalization of healthcare services and the cybersecurity issues related to patient health records and their rights to protect it. Owing to Covid-19 when the whole world transforms all their sectors in digital platform patients are not connect with the technology easily as they prefer traditional mode of visiting the doctors for their health issues. As all the patients are helpless because of deadly Corona virus several conventions and legislations appear in order to safeguard patient rights like Information Technology Act, Intellectual Property, clinical establishment Act, IMC Regulation 2002, Drugs and Cosmetics Act of 1940, Pharmacy Act 1948 etc. These entire regulations are there to ensure the availability and accessibility of healthcare services during the COVID 19 pandemic scenario, and it has necessitated a serious approach towards the Digitalization of health care services.

References

[1] B. D. Johnson, “Secret Science Fiction,” Computer, vol. 46, no. 5, pp. 105–107, May 2013, doi: 10.1109/MC.2013.180.

[2] “Future Hospital Commission,” RCP London, Sep. 16, 2013. https://www.rcplondon.ac.uk/projects/outputs/future-hospital-commission (accessed Mar. 26, 2022).

[3] “NitiAayogBook_compressed_1.pdf.” Accessed: Mar. 26, 2022. [Online]. Available: https://www.niti.gov.in/sites/default/files/2019-11/NitiAayogBook_compressed_1.pdf

[4] N. Fullman et al., “Measuring performance on the Healthcare Access and Quality Index for 195 countries and territories and selected subnational locations: a systematic analysis from the Global Burden of Disease Study 2016,” The Lancet, vol. 391, no. 10136, pp. 2236–2271, Jun. 2018, doi: 10.1016/S0140-6736(18)30994-2.

[5] A. De Mauro, M. Greco, and M. Grimaldi, “A formal definition of Big Data based on its essential features,” Libr. Rev., vol. 65, no. 3, pp. 122–135, Jan. 2016, doi: 10.1108/LR-06-2015-0061.

[6] “9789241550505-eng.pdf.” Accessed: Mar. 26, 2022. [Online]. Available: http://apps.who.int/iris/bitstream/handle/10665/311941/9789241550505-eng.pdf?ua=1

[7] “Transforming healthcare: policy discourses of IT and patient-centred care | SpringerLink.” https://link.springer.com/article/10.1057/ejis.2014.40 (accessed Mar. 26, 2022).

[8] J. Vora, P. DevMurari, S. Tanwar, S. Tyagi, N. Kumar, and M. S. Obaidat, “Blind Signatures Based Secured E-Healthcare System,” in 2018 International Conference on Computer, Infor-

mation and Telecommunication Systems (CITS), Jul. 2018, pp. 1–5. doi: 10.1109/CITS.2018.8440186.

[9] R. Wootton et al., "Long-running telemedicine networks delivering humanitarian services: experience, performance and scientific output," Bull. World Health Organ., vol. 90, no. 5, pp. 341-347D, May 2012, doi: 10.2471/BLT.11.099143.

[10] "The inevitable application of big data to health care - PubMed." https://pubmed.ncbi.nlm.nih.gov/23549579/ (accessed Mar. 26, 2022).

[11] "national_health_policy_2017.pdf." Accessed: Mar. 26, 2022. [Online]. Available: https://www.nhp.gov.in/nhpfiles/national_health_policy_2017.pdf

[12] "Disha Bill, 2019," Drishti IAS. https://www.drishtiias.com/daily-updates/daily-news-analysis/disha-bill-2019 (accessed Jun. 04, 2022).

[13] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD." https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed Mar. 26, 2022).

[14] "Liu, B.H., He, K.L. and Zhi, G. (2018) The Impact of Big Data and Artificial Intelligence on the Future Medical Model. Journal of Life and Environmental Sciences (PeerJ), 39, 1-4. - References - Scientific Research Publishing." https://www.scirp.org/(S(czeh2tfqyw2orz553k1w0r45))/reference/referencespapers.aspx?referenceid=2792392 (accessed Jun. 01, 2022).

[15] G. Sageena, M. Sharma, and A. Kapur, "Evolution of Smart Healthcare: Telemedicine During COVID-19 Pandemic," J. Inst. Eng. India Ser. B, vol. 102, no. 6, pp. 1319–1324, Dec. 2021, doi: 10.1007/s40031-021-00568-8.

[16] E. M. Strehle and N. Shabde, "One hundred years of telemedicine: does this new technology have a place in paediatrics?," Arch. Dis. Child., vol. 91, no. 12, pp. 956–959, Dec. 2006, doi: 10.1136/adc.2006.099622.

[17] S. Tian, W. Yang, J. M. L. Grange, P. Wang, W. Huang, and Z. Ye, "Smart healthcare: making medical care more intelligent," Glob. Health J., vol. 3, no. 3, pp. 62–65, Sep. 2019, doi: 10.1016/j.glohj.2019.07.001.

[18] Aqeel-ur-Rehman, I. U. Khan, and Sadiq ur Rehman, "A Review on Big Data Security and Privacy in Healthcare Applications," in Big Data Management, F. P. García Márquez and B. Lev, Eds. Cham: Springer International Publishing, 2017, pp. 71–89. doi: 10.1007/978-3-319-45498-6_4.

[19] A. Almutairi, R. AlBukhary, and J. Jayaprakash, "Security and Privacy of Big Data in Various Applications," Int. J. Big Data Secur. Intell., vol. 2, pp. 21–26, Jun. 2015, doi: 10.21742/ijbdsi.2015.2.1.03.

[20] W. Raghupathi and V. Raghupathi, "Big data analytics in healthcare: promise and potential," Health Inf. Sci. Syst., vol. 2, p. 3, Feb. 2014, doi: 10.1186/2047-2501-2-3.

[21] L. Fernandes, M. O'Connor, and V. Weaver, "Big data, bigger outcomes: Healthcare is embracing the big data movement, hoping to revolutionize HIM by distilling vast collection of data for specific analysis," J. AHIMA Am. Health Inf. Manag. Assoc., vol. 83, pp. 38–43; quiz 44, Oct. 2012.

[22] D. Houlding, "Health Information at Risk: Successful Strategies for Healthcare Security and Privacy," Success. Strateg., p. 8.

[23] "UNC Health Care Uses IBM Analytics To Manage Medical Data And Improve Patient Care." https://www.prnewswire.com/news-releases/unc-health-care-uses-ibm-analytics-to-manage-medical-data-and-improve-patient-care-227376421.html (accessed Jul. 31, 2022).

[24] R. Wyber, S. Vaillancourt, W. Perry, P. Mannava, T. Folaranmi, and L. A. Celi, "Big data in global health: improving health in low- and middle-income countries," Bull. World Health Organ., vol. 93, no. 3, pp. 203–208, Mar. 2015, doi: 10.2471/BLT.14.139022.

[25] A. Al-Shomrani, F. Eassa, and K. Jambi, "Big Data Security and Privacy Challenges," vol. 6, no. 1, p. 7, 2018.

[26] N. Upadhyay and A. Kumar, "A Framework based on Authentication and Authorization to ensure Secure Data Storage in Cloud."

[27] S. Pandey and R. Pandey, "Medical (Healthcare) Big Data Security and Privacy Issues," vol. 9, no. 2, p. 3, 2018.

[28] D. Mondek, R. B. Blažek, and T. Zahradnický, "Security Analytics in the Big Data Era," in 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Jul. 2017, pp. 605–606. doi: 10.1109/QRS-C.2017.136.

[29] "FIPS 197, Advanced Encryption Standard (AES)," p. 51.

[30] R. Zhang and L. Liu, "Security Models and Requirements for Healthcare Application Clouds," in 2010 IEEE 3rd International Conference on Cloud Computing, Jul. 2010, pp. 268–275. doi: 10.1109/CLOUD.2010.62.

[31] "FIPS 197, Advanced Encryption Standard (AES).pdf." Accessed: Jul. 31, 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf

[32] S. Fluhrer, I. Mantin, and A. Shamir, “Weaknesses in the Key Scheduling Algorithm of RC4,” in Selected Areas in Cryptography, vol. 2259, S. Vaudenay and A. M. Youssef, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 1–24. doi: 10.1007/3-540-45537-X_1.

[33] J. Shafer, S. Rixner, and A. L. Cox, “The Hadoop distributed filesystem: Balancing portability and performance,” in 2010 IEEE International Symposium on Performance Analysis of Systems & Software (ISPASS), Mar. 2010, pp. 122–133. doi: 10.1109/ISPASS.2010.5452045.

[34] “Privacy and Big Data [Book].” https://www.oreilly.com/library/view/privacy-and-big/9781449314842/ (accessed Jul. 31, 2022).

[35] M. Jensen, “Challenges of Privacy Protection in Big Data Analytics,” in 2013 IEEE International Congress on Big Data, Jun. 2013, pp. 235–238. doi: 10.1109/BigData.Congress.2013.39.

[36] “Regulation 2016/679 - Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) - EU monitor.” https://www.eumonitor.eu/9353000/1/j4nvk6yhcbpeywk_j9vvik7m1c3gyxp/vk3t7p3lbczq (accessed Aug. 01, 2022).

[37] “Data Breaches: In the Healthcare Sector,” CIS, Oct. 10, 2016. https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (accessed Aug. 01, 2022).

[38] M. M. Kavanagh, S. D. Baral, M. Milanga, and J. Sugarman, “Biometrics and public health surveillance in criminalized and key populations: policy, ethics, and human rights considerations,” Lancet HIV, pp. S2352-3018(18)30243–1, Oct. 2018, doi: 10.1016/S2352-3018(18)30243-1.

[39] “Contact Tracing Apps: Extra Risks for Women and Marginalized Groups – Health and Human Rights Journal.” https://www.hhrjournal.org/2020/04/contact-tracing-apps-extra-risks-for-women-and-marginalized-groups/ (accessed Aug. 01, 2022).

[40] “(Sort of) Trust but Verify: Palantir Responds to Questions about its work with NHS,” Privacy International. http://privacyinternational.org/long-read/3751/sort-trust-verify-palantir-responds-questions-about-its-work-nhs (accessed Aug. 01, 2022).

[41] N. Sun, K. Esom, M. Dhaliwal, and J. J. Amon, “Human Rights and Digital Health Technologies,” Health Hum. Rights, vol. 22, no. 2, pp. 21–32, Dec. 2020.

[42] “IEEE Xplore Full Text PDF.” Accessed: Jul. 31, 2022. [Online]. Available: https://ieeexplore.ieee.org/stampPDF/getPDF.jsp?tp=&arnumber=8004394&ref=aHR0cHM6Ly9pZWVleHBsb3JlLmllZWUub3JnL2RvY3VtZW50LzgwMDQzOTQ=