PRIVACY AND PROTECTION OF PATIENT SENSITIVE DATA IN THE HEALTHCARE SECTOR: A CRITICAL ANALYSIS

A thesis submitted to the

UPES

For the award of
Doctor of Philosophy
in

Law

BY

Rajesh Kumar

September 2024

SUPERVISOR

Dr. Kanchal Gupta

School of Law

UPES

Dehradun 248007: Uttarakhand

PRIVACY AND PROTECTION OF PATIENT SENSITIVE DATA IN THE HEALTHCARE SECTOR: A CRITICAL ANALYSIS

A thesis submitted to the

UPES

For the award of

Doctor of Philosophy

in

Law

By
Rajesh Kumar
(Sap ID: 500089650)

September 2024

SUPERVISOR
Dr. Kanchal Gupta
Associate Professor
School of Law, UPES

School of Law

UPES

Dehradun 248007: Uttarakhand

DECLARATION

I **Rajesh Kumar** hereby declare that the thesis entitled ***Privacy and Protection of Patient Sensitive Data in the Healthcare Sector: A Critical Analysis*** has been prepared by me based on original research under the guidance of Dr. Kanchal Gupta, Associate Professor of School of Law, UPES, Dehradun. I further declare that No part of this thesis has formed the basis for the award of any degree or fellowship previously.

Rajesh Kumar (Sap Id: 500089650)

School of Law,

UPES.

Dehradun 248007: Uttarakhand

UPES
UNIVERSITY OF TOMORROW

Great Place To Work. Certified FEB 2023 – FEB 2024 INDIA

CERTIFICATE

I certify that **Mr. RAJESH KUMAR** has prepared his thesis entitled, ***Privacy and Protection of Patient Sensitive Data in the Healthcare Sector: A Critical Analysis*** for the award of a Ph.D. degree from the UPES, under my guidance. He has carried out work at the Department of School of Law, UPES.

Supervisor

Dr. Kanchal Gupta

School of Law,

UPES.

Dehradun 248007: Uttarakhand

ABSTRACT

Article 21 of Indian Constitution, Right to Life and Personal Liberty guarantees the Right of Privacy under the purview of it, and this is also confirmed by the Apex Court in the case of Justice K.S. Puttaswami V. Union of India, 2017. But the serious violation of patient's privacy and data protection can be seen in healthcare sector. In the healthcare industry, the concept of patient privacy is a basic and moral cornerstone that emphasizes the protection of private medical information and promotes patient-healthcare provider trust. Ensuring patient privacy entails maintaining the confidentiality of individual's personal health information, regardless of technology progress. It includes multiple facets, such as the secure storage and management of medical records, restricted access for authorized individuals, and the enforcement of rigorous confidentiality regulations. Healthcare sector, without technologically advanced resources, depend on traditional techniques to maintain the confidentiality and security of patient information. Due to the importance of paper-based documents, it is necessary to have careful organization and storage procedures in place to prevent unauthorized access. Face-to-face interaction takes precedence over other methods of exchanging information, emphasizing the need of private consultations and private talks. Contrariwise, the healthcare sector faced significant challenges in maintaining patient privacy, mostly due to the absence of comprehensive and consistent regulations. There was a conspicuous lack of a unified federal statute addressing the safeguarding of patient health information. This discrepancy led to varying privacy protocols among healthcare organizations and an elevated likelihood of unauthorized exposure of confidential medical data. Patients encountered difficulties in managing access to their records, while healthcare providers lacked explicit instructions on how to handle and protect patient data. The lack of a uniformly established legal framework i.e., Drugs and Cosmetics Act 1940, Indian Medical and Central Council Act 1970, Code of Medical Ethics Regulation 2002 often resulted in

conflicts regarding privacy infringements, causing patients with few options for fixing violations.

With the technological development, adoption of Electronic Health Records (EHRs) was a critical turning point in the late 20th century as technology integration started to pick up steam. The transition from conventional paper-based record-keeping to digital technologies greatly improved the efficiency of healthcare activities. It facilitated the smooth exchange of patient data among healthcare practitioners, reducing mistakes and enhancing the overall collaboration in healthcare. The integration of technology in healthcare has also introduced cutting-edge diagnostic equipment, imaging systems, and telemedicine solutions, facilitating distant consultations and enhancing the availability of medical expertise. In addition, the progress in wearable gadgets and health monitoring applications has given individuals the ability to play a more proactive part in controlling their health. Internet of Things (IoT) and Artificial Intelligence (AI) technology in the healthcare business signifies a paradigm shift, fundamentally transforming patient care, diagnostics, and overall healthcare administration. Internet of Things (IoT) gadgets, which include a variety of smart medical equipment and remote patient monitoring systems, facilitate the effortless gathering and exchange of up-to-the-minute health information. The integrated environment enables healthcare providers to easily access comprehensive patient information, resulting in enhanced accuracy in diagnosis and treatment planning. Artificial intelligence, however, is capable of processing and analysing large information at speeds that cannot be achieved by conventional approaches. This enables the discovery of valuable insights and patterns that may be used to make informed medical decisions. The combination of IoT and AI enhances predictive analytics, allowing healthcare professionals to anticipate possible health problems and take pre-emptive measures. Utilizing Internet of Things (IoT) devices, remote patient monitoring enables uninterrupted health monitoring, hence minimizing the necessity for frequent hospital visits. The incorporation of wearables technology into the healthcare sector signifies a fundamental change in how people interact with their health and overall wellness. Wearables, which include technologies such

as fitness trackers, smartwatches, and health monitoring gadgets, have become essential tools in encouraging preventive care and empowering patients. These technologies provide instantaneous monitoring of many health parameters, such as heart rate, physical activity, sleep patterns, and additional data. Wearables facilitate the gathering and transmission of data to healthcare specialists, allowing for a thorough and uninterrupted monitoring of an individual's health condition. This research examines the various concerns and challenges that exist in the healthcare sector after the adoption of technological advancements. The incorporation of new technologies that disrupt such as Internet of Things (IoT), Artificial Intelligence (AI), and Wearables into the healthcare industry has yielded various advantages, but it also presents notable legal complexities. Data privacy and security are among the primary concerns. Given the substantial volume of sensitive health data produced by these technologies, it is imperative to implement strong procedures to protect patient confidentiality. Another legal dispute concerns the ethical application of AI in healthcare decision-making. With the growing use of AI algorithms in diagnosis and treatment planning, concerns arise about the responsibility and legal culpability in case of errors or negative effects. Ensuring clear and precise regulatory frameworks and standards for the implementation of artificial intelligence in healthcare is crucial to establish accountability and safeguard the interests of both healthcare providers and patients. The utilization of wearable devices and IoT in healthcare gives rise to concerns of permission and transparency. It is imperative to provide patients with information regarding the utilization of their data, and gaining explicit consent for the gathering and sharing of data becomes paramount. The current legal framework related to patient privacy and protection of data i.e., IT Act 2000, IT Rules 2011 (SPDI), The Clinical Establishment Rule 2012, National Health Policy 2017, Drugs, Medical Devices and Cosmetics Bill 2022, and Digital Personal Data Protection Act 2023 are not competent to handle the new challenges that arise after implementing the new technology of IoT and AI in the healthcare sector. Also, the researcher conducted the empirical research to understand the behaviour of public with respect to their rights for protecting their own sensitive data. The questionnaires were prepared on 5.0 Likert scale from strongly Agree to Strongly Disagree. The objective of this questionnaire is

to gain insights into the level of awareness and perspective held by legal experts, medical professional, and legal academicians regarding the patient privacy and data protection laws particularly in relation to the implications of integrating modern technology into the healthcare sector. This questionnaire will assist the researcher in examining the current legal framework of India and assessing the necessity of implementing new reforms from the European Union and the United States. After conducting the survey, approximately 390 responses were recorded through Microsoft forms and their results is analysed by using SPSS software applying the Mean, Median, and Mode to understand the responses and their variations of responses. The stakeholder engagement is characterized by a broad composition, consisting of 5.1% doctors, 10.5% advocates, 25.9% legal scholars, and 58.5% individuals from various other backgrounds. The consensus among participants in research on privacy legislation and healthcare technology in India is that privacy is highly significant in the domains of family, relationships, and personal space. Worries regarding the susceptibility of paper-based medical records lead 89.2% of individuals to endorse technology progress, with 90.8% expressing support for Electronic Medical Record (EMR) systems. Although there is generally a favourable view of the advantages of EMR (Electronic Medical Records), there are differing viewpoints about concerns such as data security, unauthorized access, and the involvement of IoT (Internet of Things) and AI (Artificial Intelligence).

Legal frameworks need to adapt to accommodate these ever-changing situations, guaranteeing that people have authority over their health data and are knowledgeable about its possible use.

Additionally, the researcher examines the legal frameworks of the European Union and the United States and compare them to the current legal system of India related to patient privacy and protection of patient's data. Researcher thoroughly analyse the US Privacy Act 1974, Health Insurance Protection and Portability Act 1996, Children Online Privacy Protection Rule 1998, General Data Protection Regulation 2018, California Privacy Right Act 2020, and the Cyber Security Internet of Thing Act 2020. After analysing researcher suggested the best practice that India need to be Incorporated. To validate the opinion, researcher collect the empirical data for the views that India needs to adopt the best practices from EU and US. So, majority result also suggested the same. The

recommended measures target to strengthen data protection, cybersecurity, and privacy in the changing digital environment, ensuring that India's healthcare system stays strong and in line with international standards. India is at very amateur stage to develop a comprehensive data protection law that will encompass multiple sectors, including healthcare, and to avoid the complexities in the legal regime India must adopt the best practices mentioned below according to HIPAA and GDPR to make law effectively are as follows.

- Rights of Sensitive Data Protection as a Fundamental Right.
- IT Act 2000 (amendment in 2008): Following Amendment in IT Act.
    a. Definition of Sensitive Data must be included.
    b. Need for Amendment in IT Act as to Secure Electronic Records.
    c. Processing of Sensitive Data without consent.
    d. Punishment for violation of Breach of Sensitive Data.
    e. To Establish administrative authority where the user can report in the case of any sensitive data breach.
- Sensitive Personal Data Intermediary Rules 2011
- Bifurcation in the definition of 'Sensitive Personal Data'.
- Procedure of Transfer of Sensitive Data in third countries or international organizations.
- Medical Devices Rules 2017
    a. To Include the definition of Smart Medical Devices.
    b. Processing, Securing, Storage and transferring of Patient Sensitive Data
    c. Secure Processing techniques for protecting patient sensitive data.
    d. Secure Network and Information security.
    e. Storage of Patient sensitive data.
    f. Secure Access to Health Data.
    g. Right to access and exchange of patient sensitive data outside India.
- Proposals in General
    a. The Government of India must adopt the Digital Information Security in Healthcare Act (DISHA).
- IoT Cybersecurity Improvement

These are Recommendations which has given by the researcher after thorough research on this topic and may enhance the laws of privacy and data protection in India. Further the Detailed recommendations and explanation is mentioned in the Full thesis.

ACKNOWLEDGEMENT

I am profoundly grateful for the constant support, motivation, understanding, guidance, and encouragement of my Supervisor Dr. Kanchal Gupta. My research would have been impossible without her guidance to sail through the difficult phases of the work, instilling confidence, and strength to pass each stage of the research program.

I also thank Prof. (Dr.) Abhishek Sinha (Dean SOL), Dr. Shivam Joshi, Prof. RK Chopra, Dr. Yatish Pachauri, Dr. Gaurav Mittal, Dr. Shantanu Trivedi, Prof. PP Mitra, Siddharth Singh for their constant help at various stages of the research. I also thank all the key officials at my university, for allowing me the time and support to complete this thesis.

I thank all the volunteers who participated in the survey. I would like to thank all Legal Academicians, Healthcare Experts, Advocates, Data Protection Expertise, Data Analyst for sharing their views, suggestions, and recommendations.

My sincere thanks to Professor (Dr.) Shikha Dimri, Dean R & D, UPES Ph.D. program staff, UPES library Staff, IT staff, and office staff. My heartfelt thanks to my parents for their constant support and letting me complete the thesis at a time when I was most needed with them, my family, friends, students and colleagues for their help and support.

Rajesh Kumar

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

TABLE OF ABBREVIATIONS

Ambient Assisted Living	**AAL**
Assistive Care Loop Framework	**ACLF**
Adverse Drug Reaction	**ADR**
Artificial Intelligence	**AI**
All India Institute of Medical Sciences	**AIIMS**
Auxiliary Nurse Midwifes	**ANMs**
Another	**Anr.**
Amazon Web Services	**AWS**
Before Christ	**B.C**
Bluetooth Low Energy	**BLE**
Blood-Pressure	**BP**
California Consumer Privacy Act	**CCPA**
Cognitive Data Processing	**CDP**
Continuous Glucose Monitors	**CGMs**
Child Health Information	**CHI**
Capabilities Of the Internet of Medical Things	**CIoMT**
Comparative Legal Research	**CLR**
Convolutional Neural Network	**CNN**
Children's Online Protection Act	**COPPA**
Corona Virus Disease	**COVID**
Convention On the Rights of The Child	**CRC**
Clustered Regularly Interspaced Short Palindromic Repeats	**CRISPR**
Digital Information Security in Healthcare Act	**DISHA**
Digital Personal Data Protection	**DPDP**
Electrocardiogram	**ECG**
European Convention on Human Rights	**ECHR**
Electroencephalogram	**EEG**
Electronic Health Record	**EHRs**

European Union	**EU**
Food And Drug Administration Amendments Act	**FDAAA**
Food And Drug Administration Modernization Act	**FDAMA**
Food And Drug Administration Safety and Innovation Act	**FDASIA**
Ferroelectric Liquid Crystal Display	**FLCD**
Federal Trade Commission	**FTC**
Government Accountability Office	**GAO**
Gross Domestic Product	**GDP**
General Data Protection Regulation	**GDPR**
Human-Computer Interaction	**HCI**
Health, Education, And Welfare	**HEW**
Healthcare Internet of Things	**HIoT**
Health Insurance Portability and Accountability	**HIPAA**
Hospital Information Systems	**HIS**
Health Information Technology for Economic and Clinical Health	**HITECH**
Human immunodeficiency virus	**HIV**
Health Matching Account	**HMA**
International Covenant on Civil and Political Rights	**ICCPR**
International Covenant on Economic, Social, And Cultural Rights	**ICESCR**
Indian Council of Medical Research	**ICMR**
Internet Of Computers	**IoC**
Internet Of Everything	**IoE**
Internet Of Health Things	**IoHT**
Internet Of Things	**IoT**
Internet Protocol	**IP**
International Organization for Standardization	**ISO**
Independent Software Vendors	**ISVs**
Information Technology	**IT**
In Vitro Fertilization	**IVF**

Justice	**J.**
Indian Medical Council Statute	**MCA**
Medical Council of India	**MCI**
Metadata And Data Standards	**MDDS**
Medical Device User Fee and Modernization Act	**MDUFMA**
Mammography Quality Standards Act	**MOSA**
National Electronic Health Authority	**NeHA**
Others	**Ors**
Payment Card Industry Data Security Standards	**PCI-DSS**
Personal Data Protection Bill	**PDPB**
Primary Health Services	**PHCs**
Prescription Adverse Drug Event	**PRESCADE**
Research And Development	**R & D**
Radio Frequency Identification	**RFID**
Secretary's Advisory Committee on Automated Personal Data Systems	**SACPDS**
Supply Chain Management	**SCM**
Safe Medical Devices Act	**SDMA**
Reasonable Security Practices and Procedures	**SPDI**
Security And Privacy of Digital Identity	**SPDI**
Blood Oxygen Saturation Level	**SpO2**
Statistical Package for The Social Sciences	**SPSS**
Telephone Consumer Protection Act	**TCPA**
Unmanned Aerial Vehicles	**UAVs**
Universal Declaration of Human Rights	**UDHR**
Universal Health Coverage	**UHC**
United Nation	**UN**
United States	**US**
United States Dollars	**USD**

LIST OF CASES

A

A-G (Attorney General) v. Guardian Newspapers Ltd (No. 2) United Kingdom House of Lords, Oct 13,1988

Ashworth Security Hospital v. MGN Ltd, 2002

E

Eisenstadt v. Baird, 1972

F

Furniss v. Fitchett, 1958

G

Govind vs. State of Madhya Pradesh & Ors, 1975

Griswold v. Connecticut, 1965

J

Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors., 2017

K

Kharak Singh vs. State of Uttar Pradesh and Ors, 1962

M

M.P. Sharma & Ors. vs. Satish Chandra and Ors., 1954

Menes v. Mikenkovic

Mr. X vs. Hospital Z, 1998

MS v. Sweden, 1997

LIST OF STATUTES

A. **Rules, Regulations, Policies, Acts specific to INDIA.**

1. Drugs and cosmetics act 1940.
2. Rules made in 1945.
3. Drugs Control Act 1950
4. Indian Medical Council Act 1956
5. Drugs and cosmetics act as amended in 1964.
6. Indian Medical Council (Amendment) Act 1964
7. Indian Medicine and central council act 1970
8. Medical Termination of Pregnancy Act 1971
9. The Homeopathy Central Council Act, 1973
10. MTP Rule 1975
11. Mental Health Act 1987
12. Indian Medical Council (Amendment) Act 1993
13. Transplantation of Human Organ Act, 1994
14. Transplantation of Human and Tissues act, 1994
15. Indian Medical Council (amendment) act, 2001
16. Code of medical ethics regulation, 2002
17. The Drugs and Cosmetics (Amendment) Act, 2008
18. IT Act (amended 2008)
19. The Indian Medicine Central Council (Amendment) Act, 2010
20. The Clinical Establishments (Registration and Regulation) Act, 2010
21. IT Rule 2011
22. The Clinical Establishment Rules 2012
23. Indian Medical Council (Amendment) ordinance, 2016
24. National Health Policy 2017
25. Medical Device Act, 2017
26. Digital Information Security in Healthcare, Act (DISHA, [Draft for Public Consultation]) 2017 and National electronic Health Authority (NeHA) 2017

27. Personal Data Protection Bill, 2019
28. Drugs, Medical Devices and Cosmetics Bill, 2022
29. Digital Personal Data Protection Bill, 2022
30. Digital Personal Data Protection Act 2023

B. Rules, Regulations, Policies, Acts specific to United States and Europe.

1. Pure Food and Drugs Act 1906
2. Federal Food, Drug and Cosmetic Act 1938
3. Public Health Service Act 1944
4. Radiation Control for Health and Safety Act 1968
5. Medical Device Amendments to Food Drug and cosmetics act 1976.
6. Safe Medical Devices Act (SDMA) 1990
7. Mammography Quality Standards Act (MOSA) 1992
8. Food and Drug Administration Modernization Act (FDAMA) 1997
9. Medical Device user Fee and Modernization Act (MDUFMA) 2002
10. Food and Drug Administration Amendments Act (FDAAA) 2007
11. Food and Drug Administration Safety and Innovation Act (FDASIA) 2012
12. 21st Century Cure Act 2016
13. US Privacy act 1974
14. Health Insurance Protection and Portability Act 1996
15. Children Online Privacy Protection Act 1998
16. General Data Protection Regulation 2018
17. California Privacy Right act, 2020
18. Cyber Security Internet of Things (IoT) Act 2020

CHAPTER 1
INTRODUCTION

The healthcare industry has experienced a significant shift in its operations and practices due to the ongoing trend of digitizing healthcare workflows and transitioning to electronic patient information. The volume of electronically available clinical data is expected to experience a significant growth in terms of its complexity, diversity, and timeliness. The healthcare sector generates a substantial volume of data daily, amounting to billions of tons. The worries over the security and privacy of sensitive information have been consistently developing over the years due to many emerging trends in the healthcare industry. These developments include clinician mobility and the utilization of wireless networking, advanced healthcare devices, the implementation of health information exchange systems, and the adoption of cloud computing technologies, among others. In addition, healthcare companies have discovered that relying solely on a reactive, grassroots, technology-focused methodology for identifying security and there is no legal framework that regulates the new issues arising after the advancement of healthcare sector. To protect the patient's privacy and their data is always a challenge. In this chapter, researchers present the problem that the nation is faced after the development of healthcare sector. Also, analyse and discussed the regulatory mechanism of European Union (EU), United States (US) and India. How these countries put forward to dealing with the issues of patient sensitive data and the guidelines for the manufacture of smart medical devices. Lastly, researcher also describe the gaps in Indian legal framework that need to fulfil by adopting the best practices from EU and US.

1.1. Jurisprudential aspect of Privacy

Consensus among sociologists and psychologists that individuals possess an inherent and essential requirement for privacy. The concept of an individual's right to privacy encompasses the notion that said individual should possess

authority over their personal information and be able to engage in personal matters with minimal interference from unwelcome intrusion. Privacy is a fundamental aspect that underpins our democratic principles. The preservation of privacy is of great importance to individuals, as it fosters dignity, self-determination, and individual autonomy, and ultimately contributes to the development of a more robust and engaged citizenry.

Privacy, when compared to other human rights listed in the international catalog, is difficult to establish a single and precise definition.

Despite the diligent efforts made by jurists, scholars, and theorists to establish a comprehensive definition of privacy, a state of ambiguity persists regarding its precise connotation and extent. One of the challenges lies in the expansive nature of the concept, as well as its inclination, which results in a lack of clarity that diminishes its impact in political discussions.

The global interest in the right to privacy experienced a notable surge during the 1960s and 1970s, coinciding with the emergence of information technology(Holvast, 2008). However, it is important to acknowledge that the concept of the right to privacy has deep historical, cultural, and religious roots that contribute to the widespread recognition and protection of privacy across different societies.

The historical origins of the concept of privacy can be traced back to prominent philosophical discussions, particularly Aristotle's differentiation between the public sphere of political engagement and the private sphere associated with familial and domestic affairs. Lord Denning(S. Lee, 2015) has articulated the need to recognize the 'right to privacy' with this the concept of right to confidence recognizes for all correspondence and communications which expressly or impliedly are given in confidence.

1.1.1. Different aspects of Privacy

The concept of "privacy" is complex and has wide-ranging ramifications across different sectors of society, such as the legal, social, and technological realms. fundamentally, Privacy encompasses the entitlement of individuals to maintain the confidentiality of their personal information, communications, and actions. The recognition of this right is widespread across various legal

systems and international conventions, highlighting its fundamental nature. The concept of privacy is defined differently across several domains, such as:

i. Privacy in case of Trespass: In the context of trespassing, privacy commonly pertains to an individual's entitlement to the undisturbed enjoyment of their property, free from the encroachment or intrusion of unauthorized individuals. Trespass, in its conventional interpretation, is to a legal tort that pertains to the illegal access or interference with the land or property of another individual(Farber, 2016).

ii. Privacy in terms of Press: The interplay between privacy and the press necessitates a nuanced equilibrium. From a certain perspective, it can be argued that individuals possess an inherent entitlement to privacy, which implies that specific personal details ought to be kept confidential unless voluntarily disclosed(Emerson, 1979). However, it is important to note that the press performs a crucial and indispensable function in democratic societies through the dissemination of information to the public. Furthermore, the press is granted specific freedoms that enable it to report on matters that are of public concern and importance.

iii. Privacy via Photographs: The realm of photography and its relationship with privacy is multifaceted, particularly in the contemporary digital era, wherein the rapid and extensive dissemination of photographs is made possible(Coleman, 2005). The protection of the right to capture photographs, especially in public spaces, is commonly safeguarded as a manifestation of expression or freedom of speech in numerous legal regimes. Nonetheless, this entitlement frequently gives rise to clashes with the individual's right to privacy.

iv. Privacy within the Family: The notion of privacy within the context of family is a complex construct that covers various dimensions, including physical, emotional, and informational barriers. Even within the context of familial relationships, individuals continue to uphold their unique identities and, as a result, their entitlement to personal privacy(Cahn, 1998).

v. Privacy in the Healthcare Sector: The protection of patient privacy is a fundamental principle in contemporary healthcare systems and ethical frameworks. The importance of upholding patient privacy cannot be

overstated, as it not only safeguards the rights and dignity of individuals, but also plays a key role in fostering trust in healthcare professionals and institutions(N. Shen et al., 2019).

1.2. A paradigm shifts from 'Privacy' to 'Data.'

The age of technology has experienced a significant transformation in the conceptualization of privacy, with a notable movement towards the prominence of data. Historically, the concept of privacy has been seen as the entitlement to seclusion, the freedom to avoid external observation, and the ability to choose when and with whom to disclose personal information. Nevertheless, considering the proliferation of the internet, social media platforms, and pervasive data gathering techniques, the prevailing viewpoint has evolved towards a more intricate comprehension that revolves around data. In contemporary times, the focus has shifted away from the state of being disconnected from the outside world and has instead turned towards the apprehension around the collection, storage, processing, and dissemination of personal data. Fundamentally, there has been a transformation in the dynamics of power, transitioning from exerting control over personal physical spaces to exerting control over the data that embodies an individual's digital identity. The focus has shifted from the concept of "privacy" to that of "data-sovereignty", acknowledging that in the present era, data not only encompasses our individuality but also significantly shapes our decisions, possibilities, and liberties.

1.2.1. Assimilation of technology in different Industries

The inducement of technology across various sectors has been both transformative and groundbreaking. In *healthcare*, innovations such as telemedicine and wearable technology have revolutionized patient care, offering remote consultations and real-time health monitoring. The *financial sector*, buoyed by fintech advancements, has seen the emergence of blockchain, cryptocurrencies, and robo-advisors, redefining traditional banking and investment practices. The *automotive industry* is undergoing a paradigm shift with the proliferation of electric vehicles and the advent of autonomous driving technologies, heralding a new era of sustainable and self-

driven transportation. Meanwhile, *agriculture*, often perceived as traditional, has embraced precision farming where IoT devices, sensors, and drones optimize resources and crop yields, and gene-editing techniques like CRISPR promise enhanced resistance and productivity. Across the board, the integration of technology has reshaped industries, paving the way for efficiency, innovation, and a more interconnected global economy.

1.3. Introduction to Healthcare

The health of individuals contributes to the overall well-being of a nation. Despite the progress made in healthcare in India, it still lags its international equivalents. With appropriate attention and concentration, the sector possesses the capacity to foster direct or indirect GDP development. The pursuit of a life devoid of illness and the desire for good health, characterized by the absence of ailments and a reasonably long lifespan, are important focal points in the field of healthcare. In a similar vein, the transition from a state characterized by high morbidity and mortality rates to one in which individuals lead healthy lives devoid of diseases and experience overall well-being is a highly desirable condition for society. Therefore, it is inherent that measures pertaining to health and longevity, as well as measures that encompass the demographic considerations of a society, hold significant importance within the framework utilized for assessing the development process within the human development approach(Nations, 2002). In India, the term “Healthcare” is commonly linked to hospitals, although it encompasses various components such as diagnostic centers, neuro rehabilitations, hospitals, critical care units, operating theater equipment, ancillary centers, health insurance, telemedicine healthcare software, medical tourism, and medical equipment. The healthcare industry has witnessed the adoption of numerous novel instruments and procedures. This novel technological advancement has greatly transformed the operational landscape of the healthcare industry, offering many benefits and support in various capacities. The utilization of cutting-edge technology has been shown to enhance the precision of diagnostic procedures, streamline workforce requirements, expedite patient treatment through online modalities, and yield cost savings.

In addition to the numerous advantages, the business also confronts a distinct set of issues pertaining to patient privacy and the security of patient data.

1.3.1. Wearable devices in Internet of Things (IoT) and healthcare sector

In recent years, the Internet of Things (IoT) has gained significant prominence as a leading technological innovation in the 21st century. This can be attributed to the widespread utilization of IP-based networking, increased connection across networks, favorable economics in computing, advancements in data analytics, and the emergence of cloud computing. In the healthcare industry, the utilization of Internet of Things (IoT) technology is crucial for enhancing both the efficacy and the treatment procedures for patients. The introduction of Internet of Things (IoT) technology has resulted in notable enhancements in various aspects of the healthcare industry, including patient safety, hospital resource management, and environmental monitoring such as humidity and temperature control. In the field of healthcare, the integration of Internet of Things (IoT) devices has emerged as a significant advantage for patients. These captivating and cutting-edge IoT gadgets, such as warbles, offer patients the ability to gain insights about their health status. This technology seems particularly relevant in the healthcare sector, as it facilitates continuous monitoring of medical conditions in real time. The healthcare industry encompasses a diverse array of applications for the Internet of Things (IoT). Internet of Things (IoT) enabled technologies to gather and transmit human health data in real-time. Medical records are commonly maintained in cloud-based systems and shared with authorized individuals, enabling convenient access to the information irrespective of geographical location, time constraints, or device used. Wearable gadgets and other home monitoring technologies help physicians and personal nurses monitor their patients' health status. These gadgets are equipped with Internet of Things (IoT) sensors, which enable physicians to efficiently monitor the medical diagnostic state of patients, strategize their recovery and timetable, and promptly attend to patients in need of urgent medical attention. The Internet of Things (IoT) facilitates the seamless documentation of patient’s historical medical records and prospective medical interventions.

In the entire research, the researcher mainly focuses on the wearable and technology related to wearable that used in the healthcare sector. Wearables are being used for self-monitoring and preventing health conditions such as hypertension and stress. The integration of wearable technology within the healthcare industry has emerged as a revolutionary instrument that benefits both healthcare practitioners and individuals. Conventional fitness trackers and smartwatches, exemplified by prominent brands like Fitbit, Apple, and Samsung, serve the dual purpose of tracking everyday physical activity and offering sophisticated features such as heart rhythm analysis and ECG capabilities. Continuous glucose monitors (CGMs) provide individuals with diabetes with the ability to monitor their glucose levels in real-time, thereby enhancing the efficiency of disease management. In the present era, advancements such as wearable blood pressure monitors and ECG monitors have provided patients with the ability to continuously monitor their cardiac health, granting them a sense of empowerment. Smart clothing, which is integrated with biometric sensors, provides a convenient means of monitoring physiological characteristics such as heart rate and respiration rate in a continuous and uninterrupted manner. Sleep monitors are highly valuable tools that offer significant insights into sleep patterns, facilitating the identification and effective therapy of sleep disorders. In addition, the significance of equipment such as pulse oximeters has been heightened, as they possess the capability to assess blood oxygen levels, a crucial parameter particularly relevant in times of health emergencies like the ongoing COVID-19 epidemic. Pain relief wearables and smart patches are a novel domain that harnesses technological advancements to facilitate precise pain management and provide medication. Furthermore, the utilization of specialized wearable devices, such as smart glasses designed for those with visual impairments and hearing aids combined with artificial intelligence, is significantly augmenting the overall well-being of numerous individuals. Considering the ongoing expansion of the technical domain, it is imperative to prioritize the maintenance of data accuracy, privacy, and security to effectively incorporate it into the wider healthcare sector.

1.4. Statement of the Problem

The use of technology to attend to ever-increasing health-related concerns is common and almost the same in all countries. The application of technology in health care has benefitted crores of people but also made them vulnerable by breaching their privacy and damaging many instances. Maintenance of records of patients is shifted to the electronic form of records by the introduction of new technology i.e., Internet of Things (IoT) in the healthcare sector. IoT provides better medical treatment schemes for patients with smart, automatic, timely, and emotion-aware clinical services. In COVID-19, doctors diagnosed the patients through remotely controlled medical equipment and monitor the quarantined patients through their IoT devices. IoT wearables consist of sensors and these Wearable-Sensor collect information including heart rate, body temperature, blood pressure, blood sugar, stress, consciousness, pulse counter, and accelerometer. All the data generated from devices are stored in electronic mode in the healthcare industry. This record could be subjected to the threat of security attacks, leakage, tampering, and forgery during medical data transmissions, data storage, and sharing based on public networks and cloud environments. There are various instances in India where patient data is breached, a massive data breach where over 120 million Indian patients' medical details have been leaked and made freely available on the Internet(Sen, 2020).

According to an IBM report, the average cost of a data breach in 2019 was $3.92 million, while a healthcare industry breach typically costs $6.5 million(*IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years*, 2019). The healthcare industry particularly is being targeted by attackers making it vulnerable and data breaching of patients. Electronic Medical data is more sensitive as compared to other types of data because any data tampering can lead to wrong treatment that can become fatal to life and irreversibly loss to patients. Therefore, data privacy and data protection have become serious concerns for both patients and organizations.

This sector is not governed specifically by any specialized law but to a limited extent governed under IT Law, 2000 (amended in 2008), IT Rule, 2011, and Digital Personal Data Protection Act, 2023, etc.) which are not sufficient to

deal with the issues and challenges due to technological advancement in the healthcare sector. These laws are lacking to cater to the needs of technological advancement in the healthcare sector. During the pandemic, Covid-19's use of technology shifted that relied on extensive usage of IoT. There are many IoT devices introduced in the healthcare sector that helps to sense the medical conditions of the patients such as blood pressure, oxygen level, heartbeat, and temperature, remotely diagnose the patients, control the medical equipment, and monitor the quarantined patients through their digital devices, etc. But these lead to the production of a massive amount of sensitive data and these data attract the attacker to compromise the IoT devices, manipulating the EMR of a patient may lead to cause the death of a patient. Due to the emergent need for technology, there is also a need to develop the law so that accountability of wrongdoers is fixed, and the patient gets compensation in a timely manner by examining the existing legislation in detail and suggesting changes to fill the gap. Through this study, the researcher will analyze the legal framework, policies, and other guidelines pertaining to sensitive data protection at national and global and come up with findings and suggestions for a logical solution.

The research design considered for by the researcher is qualitative combining systematic literature review, content analysis and comparative analysis of Indian Laws dealing with Electronic Medical Record Protection in Contrast to the existing European Union (EU) and United States (US) Legal Framework.

1.5. Literature Review

1.6.1. Articles/Research Papers

1. Shilpa Mandke, Komal Kudave, Rakshanda Labde, Principal Dr.J. W. Bakal, IOT based Infant Health Monitoring System, 2018(Mandke et al., 2018)

   In this work the researchers propose a capable health monitoring system for infants, with wireless communication based on IoT technology. A prototype is developed which gives a reliable and efficient baby monitoring system that can play a vital role in providing better infant care. The researchers discussed

the benefits of IoT system give a peace of mind to loved ones when they are away from their infant as they can get an update status of their well beings.

2. Sahana S Khamitkar, Prof. Mohammed Rafi, IoT based System for Heart Rate Monitoring, 2020(Sahana S Khamitkar, 2020).

   This study examines the development of a Heart Rate Monitoring system utilizing Internet of Things (IoT) technology. The primary aim of this system is to detect the patient's heartbeat, enabling the monitoring of heart attack risks and facilitating regular checkups. Monitoring the health of our bodies is of utmost importance to ensure our overall well-being. The authors provide a detailed account of the development of an affordable heart rate monitoring gadget that utilizes Bluetooth technology and is worn on the fingertips.

3. Tanzila Sabaa, Khalid Haseebb, Imran Ahmedc, Amjad Rehman, Secure and energy-efficient framework using Internet of Medical Things for e-healthcare, 2020(Saba et al., 2020).

   Internet of Things (IoT) devices establish an interconnected network that facilitates the monitoring of many medical parameters, including blood pressure, oxygen saturation, heart rate, and body temperature. These devices are designed to promptly respond to critical situations by implementing necessary interventions. The transmission of sensitive patient data over the insecure Internet exposes it to potential security vulnerabilities. The framework proposed by the researchers demonstrates enhanced performance in various aspects of medical systems for network throughput, including an 18% improvement in throughput, a 44% reduction in packet loss rate, a 26% decrease in end-to-end delay, a 29% reduction in energy consumption, and a 48% decrease in connection breaches compared to other existing solutions in the field.

4. Ameya Bondre, Soumitra Pathare and John A. Naslund, Protecting Mental Health Data Privacy in India: The Case of Data Linkage with Aadhaar, 2021(Bondre et al., 2021)

   This paper discussed about the importance of patient sensitive data and rules regulation relating specific to Europe, India. This paper might present case studies of data breaches or compare India's approach to data privacy with that of other countries. In India there is only discussion paper that was published

by the NITI Aayog, Aadhar Card Judgment, IT Act 43A, IT Rule 2011 (rule 4,5,6 and 8) that is related to patient privacy. But in GDPR of EU guidelines that covered and discussed regulation for the protection of patient sensitive data. Also, India needs to regularize the existing framework and implement Digital Information Security in Healthcare. There is no statutory body in India that manage and stores the patient.

5. Prathamesh Churi, Ambika Pawar and Antonio-José Moreno-Guerrero, A Comprehensive Survey on Data Utility and Privacy: Taking Indian Healthcare System as a Potential Case Study, 2021(Churi et al., 2021)

   Most Indian existing legislation in lacking in the taking the consent of patient before sharing his/her data to third party. sensitive data. In India protection of patient sensitive data is always ignored and there are inadequate policies, rules, regulations for the patient sensitive data. Existing Indian legislation is still silent to answer the question: Who owns and accesses patient records and why? What type of data with what granularity level must be collected? Where must the data be stored (central warehouse or hospital)? Who can view medical records? Who is responsible for disclosing medical records? Which consent must be acquired while deleting patient records?

6. Irene Ioannidou and Nicolas Sklavos, On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications, 2021(Ioannidou & Sklavos, 2021)

   This study discusses the limitations of transferring information among IoT devices due to the inadequacy of the Internet network. The text finishes by providing an overview of the key privacy and security considerations associated with some widely used commercial fitness tracking software. The answer will not be discussed to safeguard sensitive information. The primary emphasis will be on algorithms.

7. Umesh Bodkhe and Sudeep Tanwar, Secure data dissemination techniques for IoT applications: Research challenges and opportunities, 2021(Bodkhe & Tanwar, 2021)

   This study's main objective is to examine and analyze the methods and strategies used to ensure the security of data transmission and dissemination inside the Internet of Things (IoT) ecosystem. This discussion will exclude

the topic of the Internet of Healthcare Things and will refrain from addressing the legal aspects.

8. Moustafa Mamdouha, Ali Ismail Awad, Ashraf A.M. Khalaf, Hesham F.A. Hamed, Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions, 2021(Mamdouh et al., 2021)

   The researcher discusses the capabilities of IoHT sensors in detecting physiological parameters such as heart rates and blood pressures. The potential exists for an assailant to compromise these sensors, resulting in fatal consequences for the patient. It is advisable to implement regulations for a vital network that significantly impacts human lives, such as the Payment Card Industry Data Security Standards (PCI-DSS) and the Health Insurance Portability and Accountability Act (HIPAA). There are various forms of attacks that can have detrimental effects on the Internet of Health Things (IoHT) system. These attacks can result in adverse consequences, including the alteration of sensitive data or information, delays in data transmission, compromised patient data monitoring, the obstruction of IoHT applications or control over IoHT devices or sensors, manipulation of user profiles, and theft of patient payment information. Encryption and algorithms have been employed as security measures to safeguard the confidentiality of patient's sensitive information. The author has put forth a proposition for a trust framework that is decentralized and based on a private blockchain. This framework is intended to be utilized in an IoHT system. The proposed approach involves the use of smart contracts to authenticate the IoHT devices at the network level.

9. Mohammad Hossein, K., Esmaeili, M. E., Dargahi, T., Khonsari, A., & Conti, M. (2021). BCHealth: A Novel Blockchain-based Privacy-Preserving Architecture for IoT Healthcare Applications,2021(Mohammad Hossein et al., 2021)

   The author places significant focus on the notion of data privacy and data security within the context of smart healthcare applications. This text discusses several aspects of healthcare management in the context of the Internet of Things (IoT). Specifically, it addresses the use of IoT devices to

provide emergency alerts to hospitals regarding patients, the handling of data by healthcare personnel, privacy concerns related to Electronic Health Records (EHRs), potential attacks on cloud storage systems, and the vulnerability of wearable sensors and patient-generated data on smartphones to cyberattacks. The comprehensive body of work does not address the legal framework pertaining to the scenario in which a data breach occurs, resulting in the death of a patient, and subsequently, the location where the patient's guardian may file a legal lawsuit.

10. Somayeh Iranpak1, Asadollah Shahbahrami, and Hassan Shakeri, Remote patient monitoring and classifying using the internet of things platform combined, 2021(Iranpak et al., 2021)

    This study focuses on implementing an effective patient monitoring system and providing appropriate medical treatment. However, it does not address the legal implications that may arise if a wearable device is targeted by a hacker, resulting in the unauthorized access and potential compromise of sensitive patient data, which could pose a significant harm to the patient's well-being.

11. Md. Anowar Hossain, Md. Ebrahim Hossain, Mohammad Anisur Rahaman, Multipurpose medical assistant robot (Docto-Bot) based on internet of things, 2021(Hossain et al., 2021)

    This paper aims to elucidate the goal and design of DOCTO-Bot. However, the potential legal ramifications following the implementation of DOCTO-Bot have not been addressed.

12. Astrid Armgarth, Sandra Pantzare, PatrikArven, Roman Lassnig, Hiroaki Jinno, Erik O.Gabrielsson , Yonatan Kife, Dennis Cherian , TheresiaArbring Sjöström, Gautier Berthou, Jim Dowling, Takao Someya, J. Jacob Wikner, GöranGustafsso, DanielT. Simon1 & Magnus Berggren, A digital nervous system aiming toward personalized IoT healthcare, 2021(Armgarth et al., 2021)

    This article introduces a range of devices and sensors, discussing their applications across numerous devices and highlighting their respective merits. This discussion will not delve into the methods and strategies employed to ensure the security and protection of cloud-based databases, nor will it explore the legal procedures associated with such databases.

13. Chenchu Xu, Zhifan Gao, Dong Zhang, Jinglin Zhang, Lei Xu, and Shuo Li, Applying Cross-modality Data Processing for Infarction Learning in Medical Internet of Things, 2021(Xu et al., 2021)

    The researcher examines several topics including the Internet of Things, cross-modality feature learning, the Two-streams framework, contrast-enhanced imaging, and Ad 29 flexible learning. In this study, the researchers prioritized the examination of technical aspects over the legal component.

14. Dinesh Visva Gunasekeran, Rachel Marjorie Wei Wen Tseng, Yih-Chung Tham and Tien Yin Wong, Applications of digital health for public health responses to COVID-19: a systematic scoping review of artificial intelligence, telehealth, and related technologies, 2021(Gunasekeran et al., 2021).

    This study focuses on the installation of a digital health application. This paper examines the legal deficiencies inherent in the application utilized within the healthcare industry.

15. Nidhi Pathak, Student,Sudip Misra, Senior, Anandarup Mukherjee, and Neeraj Kumar, HeDI: Healthcare Device Interoperability for IoT-Based e-Health Platforms, 2021(Pathak, Misra, et al., 2021).

    This study examines the shortcomings of Sensor technology and its impact on wireless connectivity due to interference. The authors propose the utilization of IP-based interoperability within a home monitoring system, employing a structural algorithm as the foundation. This paper does not address the legal concerns that arose after the introduction of wireless sensor technology in medical diagnostic devices.

16. Yin Zhang,Yi Sun, Renchao Jin, Kaixiang Lin, and Wei Liu, High-Performance Isolation Computing Technology for Smart IoT Healthcare in Cloud Environments, 2021(Zhang et al., 2021).

    The researchers conducted an analysis and put out a proposition regarding the issues associated with the implementation of Internet of Things (IoT) technology in the healthcare sector, specifically in relation to the storage of patient data within cloud-based systems. The authors have put up recommendations for future study aimed at safeguarding the privacy of patient data.

17. Haya Elayan, Moayad Aloqaily and Mohsen Guizani, Digital Twin for Intelligent Context-Aware IoT Healthcare Systems, 2021(Nikooghadam, Amintoosi, Kumari, et al., 2021).

The twin system is the focus of this endeavor to make conventional healthcare systems smarter. Additionally, this paper addresses the security and privacy challenges that arise from the storage of large volumes of data. This study does not present a comprehensive legislative framework for ensuring the protection of patient data privacy.

18. Ying Shen, Heye Zhang, Member, Yiting Fan, Alex Puiwei Lee, and Lin Xu, Smart Health of Ultrasound Telemedicine Based on Deeply Represented Semantic Segmentation, 2021(Y. Shen et al., 2021).

In this work, the researcher focused on mobile device application for the health monitoring. Not cover the legal breach incidents.

19. João Alexandre Lobo Marques, Tao Han, Wanqing Wu, João Paulo do Vale Madeiro, Aloísio Vieira Lira Neto, Raffaele Gravina, Giancarlo Fortino, and Victor Hugo C. de Albuquerque, IoT-Based Smart Health System for Ambulatory Maternal and Fetal Monitoring, 2021(J. A. L. Marques et al., 2021).

In this study, the authors propose the implementation of a maternal and fetal emergency system for activity monitoring.

20. Balasubramanian, Venki Jolfaei, Alireza, A scalable framework for healthcare monitoring application using the Internet of Medical Things,2021(Balasubramanian & Jolfaei, 2021).

In this paper, the researchers present the benefits of IoT systems in Healthcare for monitoring patients. They also proposed a framework to be used to establish an HMA with an end-to-end Assistive Care Loop Framework (ACLF) to provide a real-time alarm and assistance to monitor pregnant women. The main gap in this work is that it does not cover the legal aspect of when the connection of medical devices is lost between patient and doctor and any mishaps occur due to the network breach. In that case, the question of liability arises.

21. Roberto De Fazio, Nicola Ivan Giannoccaro, Miguel Carrasco, Ramiro Velazquez, Paolo Visconti, Wearable devices and IoT applications for

symptom detection, infection tracking, and diffusion containment of the COVID-19 pandemic: a survey, 2021(de Fazio et al., 2021).

This work gives an overview of tracing strategies and technologies for containing the COVID-19 pandemic based on IoT technologies, wearable devices, and cloud computing. In detail, the authors demonstrate the potential of radio frequency-based signal technology, including Bluetooth Low Energy (BLE), Wi-Fi, and radio frequency identification (RFID), often combined with Apps and cloud technology. This research is not focused on the breach of data from the cloud and the server's loss. There is a need to discuss the legal issue.

22. Weizhe Chen, Shunzhi Zhu, Jianmin Li, Jiaxin Wu, Chin-Ling Chen, and Yong-Yuan Deng, Authorized Shared Electronic Medical Record System with Proxy Re-Encryption and Blockchain Technology, 2021(W. Chen et al., 2021).

    This researcher works in the traditional electronic medical record system, where centralized database storage is typically used. But for the breach of data from an electronic medical record, in that case, how will the liability be decided? For the issue, the work of the researcher got silent.

23. Hanaa Fatoum, Sam Hanna; John D Halamka, MD, MS; Douglas C Sicker, Peter Spangenberg, MD; Shahrukh K Hashmi, MD, MPH, Blockchain Integration with Digital Technology, and the Future of Health Care Ecosystems: Systematic Review, 2021(Fatoum et al., 2021).

    According to the researcher's emphasis on the Internet of Things (IoT), digital data has become essential for our everyday functioning and in health care services. The sensitive nature of health care data presents several crucial issues, such as privacy, security, interoperability, and reliability, that must be addressed in any health care data management system. The researchers suggested only the blockchain method be used to make the network strong between the device and the Internet. There is no discussion on proposing a legal framework.

24. Ahmed R. Nasser, Ahmed M. Hasan, Amjad J. Humaidi, Ahmed Alkhayyat, Laith Alzubaidi, Mohammed A. Fadhel, José Santamaría and Ye Duan, IoT and cloud computing in healthcare: A new wearable device and

cloud-based deep learning algorithm for monitoring of diabetes,2021(Nasser et al., 2021).

In this work, the authors work on How AI and IoT devices used for continuous glucose monitoring (CGM) supervise the glucose level in the blood and alert the user to the type-1 Diabetes class once a certain critical level is surpassed. Cloud computing and IoT technologies are considered to implement the prediction model and combine it with the existing wearable CGM model to provide the patients with a prediction of future glucose levels.

25. Tayyaba Ilyas, Danish Mahmood, Ghufran Ahmed, and Adnan Akhundzada; Symptom analysis using fuzzy logic for detection and monitoring of covid-19 patients, 2021(Ilyas et al., 2021).

The researchers proposed a model that deploys the IoT framework to collect real-time symptom data from users to detect symptomatic and asymptomatic COVID-19 patients. Moreover, the proposed framework is also capable of monitoring the treatment response of infected people. FLCD comprises three components: symptom data collection using wearable sensors, data fusion through a Rule-Based Fuzzy Logic classifier, and cloud infrastructure to store data with a possible verdict (normal, mild, serious, or critical).

26. Mohamed Elhoseny, Navod Neranjan Thilakarathne, Mohammed I. Alghamdi, Rakesh Kumar Mahendran, Akber Abid Gardezi, Hesiri Weerasinghe and Anuradhi Welhenge, Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions,2021(Elhoseny, Thilakarathne, et al., 2021).

The researchers discussed the various functions of IoT in the healthcare system and its different functions. In the pandemic period, IoT-based technology helped healthcare tackle the situation. The researchers also highlight the privacy and security challenges after the implementation of new technology in healthcare.

27. Sahar A. El Rahman Ala Saleh Alluhaidan; Blockchain technology and IoT-edge framework for sharing healthcare services; 2021(ElRahman & Alluhaidan, 2021).

This paper covers the Internet of Things (IoT) and how it can be used in the healthcare sector to exchange patients' information. But with that, there are

many issues and challenges related to the privacy and security of the patient's confidential information or transferring this information.

28. Zeng Chen, Weidong Xu, Bingtao Wang, Hua Yu; A blockchain-based preserving and sharing system for medical data privacy; 2021(Z. Chen et al., 2021).

    The authors focused on the rapid development of information and network technology in hospital information systems (HIS). These new technologies used in the healthcare sector produce billions of tons of patient-sensitive data. However, the patient data could be subjected to the threat of security attacks, leakage, tampering, and forgery during medical data transmissions, storage, and sharing based on public networks and cloud environments. In the suggested part, the researchers proposed to design an anonymous medical data sharing scheme based on cloud servers and a proxy re-encryption algorithm to improve the security of private medical data sharing.

29. Weizhi Meng, Senior, Yong Cai, Laurence T. Yang, and Wei-Yang Chiu, Hybrid Emotion-Aware Monitoring System Based on Brainwaves for Internet of Medical Things, 2021(Meng et al., 2021).

    The researchers discussed the Internet of Medical Things (IoMT) and its application in the healthcare sector, which was developed to help collect, analyze, and transmit medical data. During the outbreak of a pandemic like COVID-19, IoMT can be useful to monitor the status of patients and detect the main symptoms remotely by using various smart sensors. However, due to the lack of emotional care in the current IoMT, it is still a challenge to reach an efficient medical process. The authors propose an emotion-aware healthcare monitoring system in IoMT.

30. Aniello Castiglione, Muhammad Umer, Saima Sadiq, Mohammad S. Obaidat, Life Fellow, and Pandi Vijayakumar, The Role of Internet of Things to Control the Outbreak of COVID-19 Pandemic, 2021(Castiglione et al., 2021).

    This work discussed COVID-19, which is the major cause of disease burden globally. So, there is a need for an urgent solution to fight against this pandemic. The Internet of Things (IoT) can transmit data without human interaction. This technology enables devices to connect in hospitals and other

planned locations to combat this situation. The researchers proposed real-time identification and monitoring of COVID-19 patients.

31. M. Poongodi, Ashutosh Sharma, Mounir Hamd, Ma Maode, Naveen Chilamkurti, Smart healthcare in smart cities: wireless patient monitoring system using IoT, 2021(Poongodi et al., 2021).

    This work suggested patient monitoring and ambulance tracking system is an efficient system used to carry out a quick thirty-second diagnosis using heartbeat, temperature, breath rate sensors to record vital patient parameters required initially by the doctors to start any treatment and remotely transmit these parameters over wireless medium to the hospital even before the ambulance is deployed.

32. Fan Yang, Qilu Wu, Xiping Hu, Jiancong Ye, Yuting Yang, Haocong Rao, Rong Ma, and Bin Hu, Internet of Things Enabled Data Fusion Method for Sleep Healthcare Applications, 2021(F. Yang et al., 2021).

    In this paper researchers discussed the Internet of Things (IoT) techniques to provide better medical treatment scheme for patients with smart, automatic, timely, and emotion-aware clinical services. One of the IoMT instances is applying IoT techniques to sleep-aware smartphones or wearable devices applications to provide better sleep healthcare services.

33. Mehedi Masud, Senior, Gurjot Singh Gaba, Salman Alqahtani, Ghulam Muhammad, Sen, B. B. Gupta, Pardeep Kumar, A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care, 2021(Masud et al., 2021).

    The researchers cover how IoMT has enabled the doctors to remotely diagnose the patients, control the medical equipment, and monitor the quarantined patients through their digital devices. But the major issues are in the part of security of IoMT devices and the breach of sensitive data during the transmission of data from one device to another. The researchers propose a lightweight and physically secure mutual authentication.

34. Daniel Ayo Oladele, Elisha Didam Markus, Adnan M Abu-Mahfouz, Adaptability of Assistive Mobility Devices, and the Role of the Internet of Medical Things: Comprehensive Review, 2021(Oladele et al., 2021).

In this work review the adaptability of assistive mobility devices and the role of the internet of medical things in terms of the acquired information for assistive mobility devices. In findings revealed that an improvement in the adaptation of assistive mobility systems would require a reduction in training time and avoidance of cognitive overload.

35. Aman Hebbale, GHR Vinay, BVN Vamsi Krishna, Jalpa Shah, IoT and Machine Learning based Self Care System for Diabetes Monitoring and Prediction, 2021(Hebbale et al., 2021).

This paper shows the World Health Organization describes 346 million people who are affected by diabetes around the world. Furthermore, the lack of a self-care system for monitoring and detecting signs at an early stage in the patient's data causes pre-diabetes or diabetes condition which remains unrevealed in more than one-third of the population and later diagnosed with diabetes. This paper presents an Internet of Things (IoT) and Machine Learning-based non-invasive self-care system which monitors blood sugar and various vital parameters to predict diabetes well before.

36. Daniel Ayo Oladele, Elisha Didam Markus, Adnan M Abu-Mahfouz, Adaptability of Assistive Mobility Devices, and the Role of the Internet of Medical Things: Comprehensive Review, 2021(Oladele et al., 2021).

In this study, the authors critically examine the flexibility of assistive mobility devices and explore the significance of the internet of medical things in relation to the acquisition of information for such devices. In the Section discussing findings and recommendations, it was observed that enhancing the implementation of assistive mobility systems necessitates a decrease in the duration of training sessions and the prevention of cognitive overload.

37. Alexandru Vulpe, Razvan Cr aciunescu, Ana-Maria Dr. Agulinescu, Sofoklis Kyriazakos, Ali Paikan and Pouyan Ziafati, Enabling Security Services in Socially Assistive Robot Scenarios for Healthcare Applications, 2021(Vulpe et al., 2021).

The authors of the study examined the data provided by the World Health Organization, which reports that approximately 346 million individuals worldwide are impacted by diabetes. Moreover, the absence of a self-care system for the surveillance and identification of early indicators in patient data

contributes to the prevalence of undetected pre-diabetes or diabetes conditions in over 33% of the population, ultimately leading to a subsequent diagnosis of diabetes. The integration of machine learning methodologies and the Internet of Things (IoT) presents a viable approach for early diabetes prediction. This study introduces a non-invasive self-care system that utilizes Internet of Things (IoT) and Machine Learning techniques to monitor blood sugar levels and other key indicators. The system aims to detect the onset of diabetes at an early stage.

38. Muhammad Imran, Umar Zaman, Imran, Junaid Imtiaz, Muhammad Fayaz and Jeonghwan Gwak, Comprehensive Survey of IoT, Machine Learning, and Blockchain for Health Care Applications: A Topical Assessment, 2021(Imran et al., 2021).

    The researcher engaged in a comprehensive analysis and evaluation of the obstacles and issues pertaining to healthcare applications that rely on machine learning and blockchain technology.

39. Farouk Boumehrez, A. Hakim Sahour, Noureddine Doghmane, Telehealth care enhancement using the internet of things Technology, 2021(Boumehrez et al., 2021).

    This study encompasses the utilization of telehealthcare, with a particular focus on the significant role played by Internet of Things (IoT) technologies. The convergence of the Internet of Things (IoT) and the field of medical research has promising prospects for enhancing the quality and efficiency of healthcare services, as well as facilitating more effective coordination of healthcare provision within both domestic and occupational settings. The authors have put out a proposition regarding the significance and implementation of a remote healthcare system that relies on Internet of Things (IoT) technology.

40. Ankita Anand, Shalli Rani, Divya Anand, Hani Moaiteq Aljahdali and Dermot Kerr, An Efficient CNN Based Deep Learning Model to Detect Malware Attacks (CNN-DMA) in 5G-IoT Healthcare Applications, 2021(Anand et al., 2021).

    This study focuses on the necessity for intelligent schemes and architectures in E-health applications to effectively address the security threats that pose

risks to the confidentiality and integrity of patient's sensitive data. The data within e-healthcare apps is stored in cloud-based systems, which are susceptible to security breaches. The researcher introduced a novel deep-learning model, CNN-DMA, to identify and classify malware attacks. The Convolutional Neural Network (CNN).

41. Gunasekaran Manogaran, Mamoun Alazab, Houbing Song, and Neeraj Kumar, CDP-UA: Cognitive Data Processing Method Wearable Sensor Data Uncertainty Analysis on the Internet of Things Assisted Smart Medical Healthcare Systems, 2021(Manogaran et al., 2021).

    This paper presents the Internet of Medical Things (IoMT) platform which serves as an interoperable medium for healthcare applications by connecting wearable sensors, end-users, and clinical diagnosis centers. This interoperable medium provides solutions for disease diagnosis; predicting and monitoring end-user health using physiological vital signs sensed wearable sensor data.

42. R. L. Priya, S. Vinila Jinny, Elderly Healthcare System for Chronic Ailments using Machine Learning Techniques- A Review, 2021(Priya & Vinila Jinny, 2021).

    The rapid influx of data in healthcare communities necessitates the timely prediction, assistance, and prevention of diseases, particularly among the elderly population. This study examines the advantages and disadvantages of several prediction models, employing both conventional and contemporary machine learning methodologies.

43. Fatima Mohsin and Wael Elmedany, A Secure Internet of Healthcare Things for tackling COVID-19, 2021(Mohsin & Elmedany, 2021).

    This paper presents a concise introduction to the Internet of Things (IoT) and the cognitive capabilities of the Internet of Medical Things (CIoMT) and the Internet of Healthcare Things (IoHT) in the context of COVID-19.

44. Farhan Ishtiaque, Sadman Rahman Sadid, Mohammed Shihab Kabir, Syeda Omia Ahalam, Md. Sharjis Ibne Wadud, IoT-Based Low-cost Remote Patient Monitoring and Management system with Deep Learning-Based Arrhythmia and Pneumonia Detection, 2021(Ishtiaque et al., 2021).

    The COVID-19 epidemic has underscored the importance of remote patient monitoring to safeguard the well-being of both patients and healthcare

professionals. Concurrently, the proliferation of the internet in the realm of medical applications has demonstrated its efficacy in facilitating remote data collecting and monitoring. The researchers put forth a cost-effective and energy-efficient patient monitoring system that aims to collect several physiological parameters, including Electrocardiogram (ECG), heart rate, blood oxygen saturation level (SpO2), and body temperature. The device is designed to transmit these data to healthcare professionals through internet connectivity.

45. Batyr Charyyev, Mo Mansouri, Mehmet Hadi Gunes, Modelling the Adoption of Internet of Things in Healthcare: A Systems Approach, 2021(Charyyev et al., 2021).

The researcher demonstrates the capacity of the Internet of Things (IoT) to revolutionize the healthcare sector. The utilization of Internet of Things (IoT) technology facilitates the establishment of interconnected monitoring systems, sensor instruments, and small detectors. These devices can gather health data in real-time, enhancing the provision of healthcare services with increased dependability. However, it is important to acknowledge that the use of IoT technology presents significant security and privacy challenges. The authors analyze how healthcare system dynamics are altered by the Internet of Things (IoT) and examine the subsequent effects of these changes on the overall rate of adoption of smart devices in the healthcare sector.

46. Nicoletta Panunzio, Giulio Maria Bianco, RFID Sensors for the Monitoring of Body Temperature and Respiratory Function: a Pandemic Prospect, 2021(Panunzio et al., 2021).

Wearable technologies have emerged as promising tools for the timely identification of infected individuals and the remote monitoring of patients in healthcare settings and residential environments during the COVID-19 pandemic. These technologies provide a decrease in direct interactions between healthcare providers and patients, hence enhancing safety measures. Currently, there is a diverse range of wearable and epidermal Radio Frequency Identification (RFID) sensors that provide individuals with many comfortable options for wireless monitoring of various physiological data.

47. J. Vijitha Ananth, Implementation of IoT and UAV Based WBAN for healthcare applications, 2021(Ananthi & Jose, 2021).

The Internet of Things (IoT) significantly influences the reception and transmission of medical data to appropriate systems within healthcare applications. Security, expedited delivery, and energy efficiency are significant considerations within the realm of wireless body area networks. The primary emphasis of this study pertains to the expeditious transfer of data between medical practitioners and patients through the utilization of Unmanned Aerial Vehicles (UAVs).

48. Fariha Tasmin Jaigirdar, Risk and Compliance in IoT-Health Data Propagation: A Security-Aware Provenance based Approach, 2021(Jaigirdar et al., 2021).

The utilization of Internet of Things (IoT) in healthcare technology has proven to be an efficient means of facilitating decision-making processes, hence offering dependable and intelligent healthcare services to individuals who are elderly or afflicted with chronic illnesses. Given the vulnerability of this valuable data to a range of security threats, it is imperative to engage in ongoing surveillance of system adherence and the detection of security vulnerabilities in the dissemination of Internet of Things (IoT) data. This necessitates the implementation of many layers of applications. This study presents a novel system model that incorporates a unique protocol for documenting and verifying evidence pertaining to security controls for data object connections inside data provenance graphs. This model's main objective is to facilitate compliance checking for security regulations in healthcare systems.

49. Mesfer Alrizq, Shauban Ali Solangi, Abdullah Alghamdi, Muhammad Ali Nizamani Muhammad Ali Memon and Mohammed Hamdi, An Architecture Supporting Intelligent Mobile Healthcare Using Human Computer Interaction HCI Principle, 2021(Alrizq et al., 2021).

Multiple monitoring devices are used to observe a patient's condition within the healthcare facility. Furthermore, following discharge from the medical facility, the patient may undergo remote monitoring, either through the utilization of body worn sensors or by employing a smartphone that is

outfitted with sensors capable of monitoring various health parameters of the user. This presents possible obstacles for the implementation of intelligent monitoring systems for a patient's health. The researcher has put forth a refined framework for intelligent mobile healthcare (mHealthcare) that is underpinned by principles of human-computer interaction (HCI) design.

50. Maria Helena da Fonseca, Fanny Kovaleski, Claudia Tania Picinin, Bruno Pedroso and Priscila Rubbo, E-Health Practices and Technologies: A Systematic Review from 2014 to 2019, 2021(da Fonseca et al., 2021).

E-health refers to a collection of technologies that are utilized through the internet to deliver healthcare services, with the aim of enhancing quality of life and streamlining healthcare provision. The researcher employs a systematic literature review process to analyze literature. The objective of this study is to examine publications published between 2014 and 2019 to ascertain prevalent e-health practices on a global scale. Additionally, the study aims to identify the primary services offered, diseases addressed, and the corresponding technology employed in facilitating e-health practices.

51. Jorge Calvillo-Arbizua,b, Isabel Román-Martínez b, Javier Reina-Tosina, Internet of things in health: Requirements, issues, and gaps, 2021(Calvillo-Arbizu et al., 2021).

IoT technology can revolutionize the healthcare sector by enabling delivery of services to patients and facilitating the real-time collection and processing of health data from sensors. This allows for informed decision-making in the healthcare domain.

52. Mohamed Elhoseny, Khalid Haseeb, Asghar Ali Shah, Irshad Ahmad, Zahoor Jan, and Mohammed. I. Alghamdi, IoT Solution for AI-Enabled PRIVACY-Preserving with Big Data Transferring: An Application for Healthcare Using Blockchain, 2021(Elhoseny, Haseeb, et al., 2021).

IoT-based technology offers an improved option for addressing issues pertaining to patients, hospitals, and healthcare professionals through the real-time diagnosis and analysis of important data. The occurrence of network disruptions caused by external entities or malicious actors, resulting in repeated instances of unauthorized access to sensitive and personal health information, undermines trust and dependence on network systems. The

researchers have put up a proposed solution in Internet of Things (IoT) for ensuring privacy while utilizing artificial intelligence (AI) and transferring large volumes of data. This proposed approach incorporates the use of blockchain technology.

53. Reeva Lederman, Ofir Ben-Assuli, Thanh Hong Vo, the role of the Internet of Things in Healthcare in supporting clinicians and patients: A narrative review, 2021(Lederman, Ben-assuli, et al., 2021).

The researchers conducted a comprehensive analysis of the factors contributing to the successful application of Internet of Things (IoT) technology in the healthcare industry. Healthcare systems must be adequately prepared to embrace the significant technical advancements and changes brought about by the Internet of Things (IoT). This entails developing suitable alliances and identifying value propositions.

54. R. Somasundaram, Mythili Thirugnanam, Review of security challenges in healthcare internet of things, 2021(Somasundaram & Thirugnanam, 2021). The researchers mentioned the services of IoT in healthcare has increased exponentially. At the same time, security issues in the system also increase this situation threatening the health and safety of patients. Implementation of smart medical device usage in the hospital like Implantable Medical Devices, Radio Frequency Identification tags, and wearable devices are prone to a severe security vulnerability. This scenario emphasizes the importance of providing privacy and confidentiality of a patient's medical information. Lastly, the authors suggested reviewing the security issues that came after the implementation of IoT devices in the health care sector.

55. Shuva Paul, Muhtasim Riffat, Abrar Yasir, Mir Nusrat Mahim, Bushra Yasmin Sharnali, Intisar Tahmid Naheen, Akhlaqur Rahman and Ambarish Kulkarni, Industry 4.0 Applications for Medical/Healthcare Services, 2021(Paul et al., 2021).

This study undertakes an analysis and identification of the various uses of the Internet of Things (IoT). What are the various advanced technologies, solutions addressing present difficulties, and pioneering start-ups that have had an influence on the healthcare sector within the context of the industry 4.0 paradigm.

56. Ashish Singh, Kakali Chatterjee, Securing smart healthcare system with edge Computing, 2021(Singh & Chatterjee, 2021).

This study discusses the emerging issues that the healthcare system encounters because of the escalating expansion of sensitive patient data. The researcher has put out a proposition for a smart healthcare system that is founded on an edge computing architecture. The architectural design incorporates an intermediary layer known as the edge computing layer, which is tasked with managing network latency and safeguarding the confidentiality of patient data.

57. Mohamed Amine Ferrag, Lei Shu, Fighting COVID-19 and Future Pandemic with the Internet of Things: Security and Privacy Perspectives, 2021(Ferrag et al., 2021).

This study examines different strategies employed to mitigate the impact of COVID-19 and other pandemics through the utilization of technological advancements, including the Internet of Things (IoT) and 5G/6G connectivity. The security of IoT devices employed for COVID-19 monitoring and treatment, specifically medical IoT devices, is of paramount importance due to the potential severe repercussions that may arise from their compromise, including life-threatening threats to patients affected by COVID-19. The survey aims to investigate IoT-related solutions, potential security, and privacy threats, as well as the corresponding requirements.

58. Nidhi Pathak, Graduate, Pallav Kumar Deb, Anandarup Mukherjee, and Sudip Misra, IoT-to-the-Rescue: A Survey of IoT Solutions for COVID-19-Like Pandemics, 2021(Pathak, Deb, et al., 2021).

This study examines potential Internet of Things (IoT) technologies that can effectively address the challenges posed by viruses such as COVID-19. This study also emphasizes the societal ramifications resulting from pandemics and outlines the specific deficiencies in existing IoT solutions. Additionally, please furnish a thorough explanation on strategies for mitigating the difficulties, as well as guidance on potential technological advancements for future investigation.

59. Priyan Malarvizhi Kumar, Choong Seon Hong Gokulnath Chandra Babu Jeeva Selvaraj Usha Devi Gandhi, Cloud- and IoT-based deep learning

technique-incorporated secured health monitoring system for dead diseases, 2021(Malarvizhi Kumar et al., 2021).

This study highlights the significance of addressing the security concerns associated with healthcare systems, given the substantial number of users and the sensitive data they possess, particularly in the context of the rapidly evolving internet era and cloud-based databases. The researchers presented a novel data storage strategy that ensures the secure storage of patient data within cloud databases. In this paper, we provide a pair of novel cryptographic algorithms designed to facilitate the encryption and decryption operations.

60. Mian Ahmad Jan, Fazlullah Khan Spyridon Mastorakis, Muhammad Adil, Gradua, Aamir Akbar, Light IoT: Lightweight and Secure Communication for Energy-Efficient IoT in Health Informatics, 2021(Jan et al., 2021).

Internet of Things (IoT) enabled devices are used in hospital and home settings to monitor patients. These devices can collect and transmitting many types of biomedical data, including but not limited to blood pressure, electrocardiography (ECG), blood sugar levels, and body temperature. The researchers have put out a proposal for Light IoT, which is a communication technique that is both lightweight and safe. This approach is designed specifically for the transmission of data among the many devices within a healthcare infrastructure.

61. Asma Channa, Nirvana Popescu, Justyna Skibinska and Radim Burget, The Rise of Wearable Devices during the COVID-19 Pandemic: A Systematic Review, 2021(Channa et al., 2021).

The healthcare infrastructure in industrialized nations, including the United States, Europe, and the United Kingdom, may be insufficiently developed or lack adequate facilities to effectively address and mitigate the challenges posed by the ongoing pandemic. There exists a pressing demand within the healthcare sector for the implementation of remote monitoring systems to track and assess symptoms associated with COVID-19. In this study, the authors presented novel approaches for the diagnosis of patients during the prodromal phase and the monitoring of symptoms, such as respiration rate, heart rate, temperature, and others. This systematic study examines the

utilization and significance of wearables within the healthcare system as assessed by the authors.

1.6.2. Books

1. Rita Marie Cain, *Global Privacy Concerns and Regulation- In the United States a world apart? 2010*(Cain et al., 2021).

   This book explains the Internet of Things (IoT) as a burgeoning worldwide system that operates on the Internet and enables the interchange of services. It highlights the steady development of IoT and its potential for rapid adoption across numerous industries. In the foreseeable future, civil society is anticipated to utilize the internet of things in a manner like its current usage, with potential expansion into sectors such as healthcare. The ramifications of the Internet of Things (IoT) will manifest in diverse domains. The legislative framework should include safeguards that effectively safeguard the security and privacy of both industries and consumers. Moreover, it is imperative to consider the legal ramifications associated with the deployment of Internet of Things (IoT) devices. The Internet of Things (IoT) has demonstrated numerous advantageous impacts across diverse sectors, encompassing developing nations in the realm of global trade, the management of agricultural businesses, the facilitation of smart homes, and the enhanced accessibility of various resources.

2. Rolf H. Weber & Romana Weber, *Internet of Things Legal Perspectives, 2010*(Weber, 2013).

   The author of this book emphasizes the difficulties associated with cyber security and concerns over privacy in the digital realm. This discussion pertains to the consequences of a data breach on customers. The decline in user interest towards advanced technology and IoT devices

3. Samant Khajuria & Lene Sorensen, *Cybersecurity and Privacy- Bridging the Gap,* 2017(Sørensen et al., 2022).

   The author draws a comparison between the existing Internet of Computers and the forthcoming iteration known as the Internet of Things. Numerous cyber assaults are perpetrated against computing devices on the Internet, and a similar trend is observed with Internet of Things (IoT) devices. To address

these concerns, it is imperative for individuals and communities to cultivate a heightened awareness. Additionally, the paper examines the technical strategies employed to mitigate assaults on the Internet of Computers (IoC).

4. Scott J. Shackelford, *The Internet of Things what Everyone needs to Know,* 2020(Shackelford, n.d.).

   This book comprehensively addresses several aspects pertaining to the Cyberworld. Beginning with its inception, cyberspace is a conceptual realm that encompasses interconnected digital networks and virtual environments. As technological advancements progress, cyberspace has evolved to incorporate a wide array of sophisticated technology. The topic of discussion pertains to the Internet of Things (IoT) and the Internet of Everything (IoE), encompassing the interconnectivity of objects through the internet. The discourse will delve into several aspects, ranging from the functionality of internet-connected devices in a working environment to the critical issue of security, specifically focusing on data breaches and security measures.

5. Colin J. Bennett, *Regulating Privacy Data Protection and Public Policy in Europe and United States,* 1992(Bennett, 1992).

   This book presents a comparative analysis of data protection policies in four countries: Sweden, the United States, West Germany, and the United Kingdom. The central focus of this study is to examine how diverse political systems have governed the collection, storage, and transmission of personal information, shedding light on their cultural, ideological, and institutional contexts. This chapter primarily concentrates on policy matters rather than addressing the challenges that arose following the integration of technology in different sectors. It does not delve into the discussion of rules and regulations necessary for effectively regulating data protection issues.

6. Ahemed Elngar & Prathamesh Churi, *Data Protection and Privacy in Healthcare Research and Innovations, 2021*(Elngar et al., 2021).

   In this study, the authors cover the security and privacy concerns of data due to rapid growth or advancement of technology. The data was produced in billions of tons daily, so the storage, transition, transfer, and processing of data is always a big challenge. Various new techniques used in healthcare for machine learning for the prediction of certain disease, IoT based healthcare

system, cloud-based healthcare system etc. Because of that the chances of privacy concerns increasing and for that there is a need for a legal framework. This book addresses the different privacy and challenges that arise after the implementation of technology in the healthcare sector.

7. Maria Tzanou, *Health Data Privacy under the GDPR Big Data challenges and Regulatory and Responses,* 2020(Tzanou, 2020).

   In this book, the researchers mainly focus on the increasing of Big Data due to the usage of technology into the routine lifestyle. In COVID time, technology is used as an alternative to tackle the patients, increasing the big data. To storing and processing data leads to security concerns for the patient's privacy. There is always a question that how the law can protect us from such egregious data misuses and what are the appropriate legal solutions to address health data surveillance. For all these issues the EU negotiated and adopted regulation (EU) 2016/679 of the EU parliament. General Data Protection Regulation 2016 was tested in the entire chapter for the search of the above questions.

8. Dac-Nhuong le & Gia Nhu Nguyen, *Emerging Technologies for Health and Medicine Virtual Reality, Augmented Reality, Artificial Intelligence, Internet of Things, Robotics, Industry 4.0*, 2018(Le et al., 2018).

   In this, the author's focuses on the advancement of technology and innovation in healthcare is rapidly expanding. As a result, many different areas of technology are getting faster and 5G mobile technology allows internet of Medical Things to greatly improve the patient care and more effectively cure the patient's disease. The study gives a review of the current and anticipated changes in medicine and healthcare due to new technologies and faster communication between patients and doctors.

1.7. Literature Gap

The above-reviewed literature covers the challenges in the protection of Electronic Medical Records (EMR) and the upcoming issues which have arisen in the health care sector; it is imperative to protect the EMR. The researchers have proposed various technical frameworks such as the implementation of strong hash function tools for protecting EMR, hash

algorithm used to secure the data and change the cloud storage system by what happens if such data is a hack or get malfunction or manipulated by the third party. However, the researchers have not highlighted much on the desired legislative framework in India to address the legal issues (breaches, attacks, manipulation of EMR, malfunction of IoT devices, etc.) and the policies that regularize the new issues in the healthcare sector. Although the General Data Protection Regulation Act has been mentioned in some of the research that will be used in regularizing and protecting sensitive data in the healthcare sector. This provides an opportunity for the present research to fill this existing literature gap by considering the Indian legislation, rules, and policies.

1.8. Need for Study

With the exponential growth of Internet-connected devices in the healthcare sector, cases of threat to confidential patient information and leakage of sensitive data to outside parties are increasing rapidly. Attackers can remotely access the control unit of the medical device (IoT) and jeopardize the lives of patients(W. Zhao et al., 2012). Recent stats indicate that with the ever-increasing cyber-attacks that target healthcare, the healthcare IoT security market is expected to undergo rapid growth by the year 2025, with total revenue of USD 100 billion, which also justifies our efforts to examine the current state of security, privacy, data protection of the IoT through this study. Researchers are no going to secure the sensitive data stored in the electronic medical records and propose robust technical solutions like using a secure AWS cloud system for storing patient data, for transmission of patient data using RFID servers, strong algorithms, etc. However, the legal issues concerning the protection of sensitive data of patients, liabilities issue, network loss, the standard for devices, etc. require a comprehensive approach to deal with all the emerging issues coming after using IoT devices. For this purpose, the development on the subject mainly in the EU and the US who are already taking care of protecting sensitive data stored in EMR and regularizing the IoT devices used in the healthcare sector will act as a benchmark to be used for comparison with the existing legal framework and to suggest analyzing guidelines to the government of India to taking care.

1.9. Research Objective

The precise objectives of the study are as follows:

- To study and analyse the issues of privacy and data protection (sensitive data) in the Healthcare Sector after the Introduction of Technology.
- To analyse the existing Indian legal framework related to Patient Sensitive Data Protection related to Electronic Medical Record in the Healthcare Sector.
- To Compare the Indian legal framework with the Europe and United States legislation and after critically analyse them, provide suitable recommendations for Patient Sensitive Data Protection in India.

1.10. Research Questions

- What are the issues and challenges prevalent in the Healthcare Sector after the introduction of technology?
- What is the legal position in India to deal with the issues of Data Protection related to Electronic Medical Records in the Healthcare Sector**?**
- What best practices can be adopted from the European Union (EU) and United States (US) legislation in India to protect the sensitive data of the healthcare sector?

1.11. Hypothesis

The existing legal framework of India is not sufficient to deal with the legal issues associated with the implementation of advanced technology in the Healthcare sector.

1.12. Research Methodology

The researcher intends to utilize the Doctrinal and Empirical method to conduct the research based on its objectives. The Doctrinal component employs a combined method involving Bibliometric-Analysis and Systematic-Literature-Review, concentrating on the Indian legal framework, policies, bills, case laws, judgments, textbooks, commentaries, and research papers. For CLR (Comparative Legal Research) involves utilizing

methodologies such as parallel studies, viewing one's own system from a foreign perspective, examining foreign systems via one's own cultural lens, and incorporating foreign theories or concepts. Law commissions and judges consider Common Law Reasoning (CLR) to be an invaluable tool for their problem-solving roles. Europe and the United States were chosen as benchmarks due to their extensive data protection legislation for regulating sensitive data. The questionnaire would be created for the empirical study using structured instruments with a 5.0 Likert scale. It will be distributed to advocates, legal academicians, and doctors in India. The data will be analyzed using the SPSS (Statistical Package for Social Sciences) software package.

CHAPTER 2

GLOBAL PERSPECTIVE OF PRIVACY LAW WITH SPECIAL REFERENCE TO THE HEALTHCARE SECTOR

2.1. Introduction

The word Privacy has been hailed as "an integral part of our humanity", the "heart of our liberty", and "the beginning of all freed"(Solove, 2016). However, the value of privacy is so complex, so entangled in competing and contradictory dimensions, and distinct meaning, that sometimes it becomes despair to usefully address it. Privacy has been used as the key term for a plethora of debates of a wide range of issues, likely to unreasonable searches of premises, clicking photographs without consent, recording private moments of couples, disclosure of secret documents to the public, in healthcare sector sharing the patient sensitive information without patient's consent, their family members, right to abortion without the consent of mother are few examples of violation of privacy in healthcare.

2.1.1. Concept of Privacy

The concept of *'privacy*' is not a new, or even relatively recent, phenomenon. Privacy has been an inherent human concern that has been valued for thousands of years. Yet while the concept of privacy has deep historical roots, personal physical and psychological privacy expectations and attributes have varied widely across societies and cultures. In the past century and one-half, the concept of privacy has expanded dramatically in the United States as the result of several simultaneous movements:

i. technological innovation that has permitted intrusion, collection, maintenance, and integration of ever smaller pieces of more disparate data on the activities and characteristics of individual citizens.
ii. the growing awareness of the concept of privacy as a fundamental individual right; and,

iii. the legal privacy response in courts and legislatures which have had the effect of structuring, expanding, and explicating the right of individual privacy.

As the quotation by Louis Henkin at the beginning of this chapter reflects, even today a concise definition of '*privacy*' has proven remarkably elusive. This is because the concept of privacy has had no common definition, no agreed upon parameters, and the many facets of privacy are deeply embedded in temporal, social, and cultural contexts. At some times, and in some cultures, privacy has even been viewed as an antisocial characteristic and a negative value because it conflicted with the public values and cohesiveness of society. The very concept of privacy has varied over time and across cultures and has grown to reflect an evolving variety of new perceived threats and incursions into the '*privacy*' of the individual over the past century. Up until the end of the nineteenth century, privacy was primarily a physical concept having to do with intimacy, concealment of the person and possessions, or the retreat of the individual relative to the outside, or public dimension. Within the past century, the concept of privacy has flourished and blossomed to encompass not only the physical domain, but also the unseen psychological and information-data domains.

Indeed, the notion of privacy is full of disarray, and hence, there is hardly any definition of privacy that can satisfy everybody. At the same time, the evaluation and justification of privacy in society plays a crucial role in rendering dimensions.

2.1.2. Privacy defined in Dictionary.

i. According to Merriam-Webster, the quality or state of being apart from company or observation or freedom from unauthorized intrusion(*Privacy Definition & Meaning - Merriam-Webster*, n.d.).

ii. According to Cambridge Dictionary, someone's right to keep their personal matters and relationships secret(*PRIVACY | Meaning, Definition in Cambridge English Dictionary*, n.d.).

iii. Privacy is a fundamental right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built(*What Is Privacy? | Privacy International*, n.d.).

2.1.3. Privacy according to different jurists

i. Ruth Gavison, for instance, shares that privacy has some constituent components, such as anonymity, solitude, and secrecy(Gavison, 1980).

ii. Helen Nissenbaum classified privacy as a dynamic and complex issue and the sensitivity to the data in terms of purpose, context, and trust(*Start Reading Privacy in Context | Helen Nissenbaum*, n.d.).

iii. Westin attempted to articulate privacy in social, personal, and regulatory dimensions(Stockdale, 2019).

iv. Anita Allen concludes that privacy appears the multifaceted denominations, e.g., physical, proprietary, decisional, informational, and so on(Allen, 2000).

v. D. W. Prosser in 1960, explained that privacy is a group of the following four torts:

- Intrusion upon the plaintiff's seclusion or solitude or into his private affairs.
- Public disclosure of embarrassing private facts about the plaintiff; publicity which places the plaintiff in a false light in the public eye; and
- Appropriation, for the defendant's advantage, of the plaintiff's name or likeness(Prosser & N, 1960).

vi. Plato, the ideal society, had no need for privacy, and this was reflected in Plato's major political treatises. In the model society Plato described in the Republic, the private sphere would be subordinated in the common community of wives, children, and education.

vii. Barrington Moore observed that although ancient Athens Greece acknowledged the public and the private domain, '*Privacy cannot be the dominant value in any society. Man must live in society, and social concerns must take precedence.*'

viii. Moore(Moore, 2008) notes that '*the words employed for private convey(ed) some hint of the antisocial in their meaning.*'

ix. The English philosopher John Locke (Nimbalkar, 2011), *privacy was one of the pre-societal or "natural rights" which was preserved when individuals, by the social contract, agreed to form a society. Furthermore,*

when society, by a second social contract, agreed to form a government, privacy was one of the rights the government was expected to preserve and protect.'

2.2. Contemporary Stages of Privacy Development

Privacy has never been a clear concept since its inception. The history of privacy can be traced back to ancient times but the rise of more modern and contemporary interpretations of privacy can be related to the periods shown in Figure 2.1.

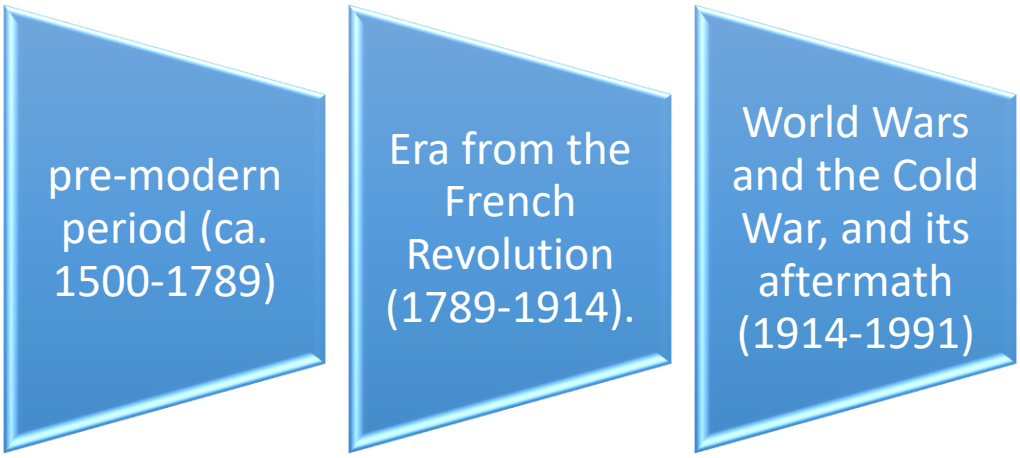

Figure 2.1 Periodization of Privacy from 1500-1991

i. **Pre-modern period (ca. 1500-1789)**

The sociologist of totalitarian regimes Barrington Moore wrote a social and cultural history of privacy in the ancient world. He emphasized that '*totalitarian' regimes throughout history have been trying to control their subjects'* lives by either denying them privacy or through surveillance. Moore, for example, looked at the Chinese Qin dynasty from 221-206 BC (*Qin Dynasty of the Ancient China (221-206 BC) | Short History Website*, n.d.) and the Indian Maurya Empire (*Maurya Dynasty (321-184 BC)*, n.d.) from 322-187 BC, and stressed how they were unsuccessful in controlling privacy as they lacked modern equipment like phone tapping or closed-circuit television (CCTV) for surveillance(Jr., 1984).

ii. **Era from the French revolution (ca.1789-1914)**

The concept of privacy is fundamentally connected to individualism and the rise of a middle class that had the freedom to pick their own living arrangements while still having the opportunity to engage in intellectual activity. These groups were not, however, the ruling classes or the lower classes (Webb, 2007).

Due to the widespread use of diaries, historian Philippe Aries claims that England towards the end of the fifteenth century was '*the origin of privacy.* Closets and the study, as well as private letters, journals, and autobiographies, gained popularity (*Theorists: Philippe Ariès*, n.d.). For those living at the time, privacy was not, however, a real boon. Shakespeare's time and works, as demonstrated by linguists and cultural historians.

In the backdrop of the growing popularity of reading in the seventeenth century, Jagodzinski (Le et al., 2018) demonstrates how the idea of privacy evolved. The circulation of printed books increased along with their number. A new sense of personal sovereignty, a new consciousness of self-began to develop in readers. This contributed to the development of the idea of privacy as a human right and the foundation of individuality. Jagodzinski claims that the practice of private spiritual reading served as the impetus for these changes since ongoing theological conflicts in post-Reformation England '*finally reaffirmed the right to individual autonomy in all things (including the religion)*'. This was an ongoing process rather than a revolutionary one(Westin, 1968). Treatises of Government (1690) of the protoliberal and philosopher John Locke(Anstey, 2011) (1632-1704) are symbolic for this new understanding of privacy as personal autonomy and individuality. In his contract theory, he contends that rational people's rightful desire to safeguard their personal lives, liberties, and property leads to cooperation in the stability of a political society.

iii. World War and the Cold War, and its Aftermath (1914-1991)(*History of Privacy Timeline*, 1980)

- **Establishment of the FTC (1914):** The Federal Trade Commission (FTC) assumes a crucial role in the preservation and implementation of privacy rights and regulations inside the United States. Since its inception in 1914, the Federal Trade Commission (FTC) has undergone a transformation in its scope

and objectives to effectively tackle the ever-changing issues posed by the digital age. Its primary aim is to enforce regulations that promote fairness and transparency in the way businesses handle consumer data. The Federal Trade Commission (FTC) has effectively taken measures to ensure accountability among various organizations by addressing instances of inadequate security measures, false privacy commitments, and infringements of the private rights of children. The Commission has played a significant role in formulating norms and regulations pertaining to data protection. Additionally, it actively engages in the dissemination of knowledge to businesses and consumers regarding the significance of privacy and the associated rights and obligations for personal data. The significance of the Federal Trade Commission's (FTC) oversight in addressing privacy concerns is increasingly paramount considering the ongoing technological advancements and the expanding digital presence of consumers.

- **Ruling on Protection of Sealed Mail 1917** (*Mail | The First Amendment Encyclopedia*, n.d.)**:** In the second decade of the 20th century, the newly established Bureau of Investigations was actively working on investigating acts of foreign sabotage and rooting out subversion. Surveillance extended to monitoring and illegally opening correspondence of suspected subversives. When the bureau filed an official request to open mail, Solicitor General Judge William Lamar ruled against the privacy infringement and upheld long-established protections of sealed mail.
- **U.N. Declaration of Human Rights (1948):** Proclaimed by the United Nations General Assembly on December 10, 1948, the U.N. Declaration of Human Rights(*Universal Declaration of Human Rights*, 1948) (UDHR) was drafted by representatives from all over the world with a variety of legal and cultural backgrounds. Article 12 states that "*No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks*." Here is the first time, where discuss privacy as a right.
- **Privacy Torts (1960):** In 1960, William L. Prosser(Prosser & N, 1960), a well-known legal scholar of the time, published the article *Privacy*. In this

article, still considered influential in the field of privacy law today, he outlined four torts that would allow someone whose privacy was violated in one of those four ways to sue the perpetrator for damages. These torts are still used today:

a. Intrusion upon seclusion or solitude, or into private affairs.
b. Public disclosure of embarrassing private facts.
c. Publicity which places a person in a false light in the public eye; and
d. Appropriation of one's name or likeness.

- **Alan Westin Writes Privacy and Freedom (1967):** Alan Westin(Westin, 1968), who defined privacy as *the claim of individuals … to determine for themselves when, how and to what extent information about them is communicated*, helped set the stage for modern debates about technology, privacy, and personal freedom. His book, Privacy and Freedom, is still one of the seminal works on privacy to this day.
- **Report of the Health Education, and Welfare Advisory Committee on Automated Personal Data Systems (1973)**: The Department of Health, Education, and Welfare (HEW) Secretary's Advisory Committee on Automated Personal Data Systems(Spark and Cannon, 2016) (SACAPDS) developed the landmark 1973 Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems. The report was the origin of Fair Information Practices, a set of principles that formed the basis for modern privacy legislation.
- **Privacy Act of 1974:** The Privacy Act of 1974(*Privacy Act*, 1974) is a U.S. federal law establishing a Code for Fair Information Practice by federal agencies. The agency's main role is to collect, maintain the records, use, and protect personally identifiable information.
- **Privacy Commission Report (1977):** Established in Section 5 of the Privacy Act of 1974, the U.S. Privacy Protection Study Commission was tasked with evaluating the Privacy Act and issuing a report containing its findings and recommendations for improvement. The Commission(*Personal Privacy in an Information Society*, 1977) issued its final report and ceased operation in 1977.

- **George Orwell Writes (1984):** George Orwell in his book emphasis on dystopian view containing themes of nationalism, futurology, censorship, and surveillance. He further states that public and private spaces are filled with cameras and microphones to penetrate privacy of an individual which is controlled by undercover agents of the government(Orwell, 1984).
- **The Telephone Consumer Protection Act and National Do Not Call Registry (1986):** The Telephone Consumer Protection Act(*Understanding the Telephone Consumer Protection Act | Insights | Greenberg Traurig LLP*, 2020) (TCPA) and the National Do Not Call Registry regulate telemarketing calling and automated telephone dialing. The TCPA prohibits certain types of solicitation calls, while the Do Not Call Registry allows consumers to opt out of telemarketing calls.
- **Common Rule Human Subject Research Privacy (1991):** In 1991, revisions were made to the U.S. Department of Health and Human Services Title 45 CFR 46 (Public Welfare) Subparts A, B, C and D. Subpart A, known as The Common Rule, is an updated version of a 1981 rule of ethics in the United States concerning biomedical and behavioral research involving human subjects. It was adopted by Institutional Review Boards for oversight of human research and is the standard of ethics guiding all government funded (and most non-government funded) research in the U.S.

  Though the word privacy is used almost everywhere, it is an uphill task to explain what privacy really entails. The notion of privacy first appeared in the famous study (The Right to Privacy) written by Louis Brandeis and Samuel Warren in 1890.(Prosser & N, 1960) They originally described the right to privacy as an already existing common law right which embodied protections for everyone's '*inviolate personality*'. Many others have since agreed that privacy is somehow fundamental to our '*personhood'*(Reiman, 1976).

  Generally, privacy must be viewed as the bundle of interests that individuals have in their personal sphere free from interference from others. There is no specific international document pertaining to human rights before 1948. After World War II in 1948 with the formation of United Nations which prepared a declaration as Universal Declaration of Human Rights (UDHR 1948) was a benchmark to all the nations which expressly include the protection of

personal information as an aspect of the right to privacy under Article 12 of UDHR. The concept of privacy has provided new insights into contemporary challenges and the history of privacy. For example, privacy has had different meanings and, as an ideal, came into existence under specific historical circumstances. Moreover, over the last 30 years, concerns about privacy and privacy regulations have influenced the profession of historians.

The evolving information age is transforming our lives in such a way that we could never imagine. In a data-based economy, privacy appears as one of the pressing concerns due to numerous reasons, such as the globalization of human communication; the commercial importance of data; the interest of governments in accessing and processing data; voluntary data sharing by people in social media; commercialization of personal data; usage of cloud computing, and recognition of privacy as one of the fundamental human rights, e.g., freedom of speech(Kuner et al., 2013). In a networked world, diverse actors always monitor or track our activities, and consequently, our privacy witnesses' tremendous threats. Indeed, privacy is indispensable, and hence, no one can violate privacy unless there remains a compelling state interest(CAHAL & CADY, 1962).

Privacy is a matter of utmost importance because we all love to have an intimate life and like to share our stories and memories with only those whom we believe. Moreover, in pure democratic culture, personal liberty includes the autonomy and freedom of individuals from the unauthorized access of business, and public and private actors. It would be disastrous if any of these actors leaked, in any way, our sensitive personal data. The losses will be unthinkable, as most of them are irreparable and admit no substitutes or compensations. Rotenberg remarked way back in 1996 that [p]privacy will be to the information economy of the next century what consumer protection and environmental concerns have been to the industrial society of the 20th century.(*Big Brother Is Us - The New York Times*, n.d.) Anticipation has widely been explicit, as privacy emerges as one of the most desired interests in the contemporary world. Thus, from the cradle to the grave, privacy requires to be duly acknowledged and respected.

2.3. Judicial Interpretation of Privacy

i. In 1928, Olmstead v. United States(*Olmstead v. United States*, 1928) known as wiretapping case, in which Justice Brandeis, dissenting, wrote broadly of the right to be "*let alone*". The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They conferred, as against the government, *the right to be let alone* the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

ii. In the case of Furniss v. Fitchett(*Furniss v. Fitchett* , 1958) is instructive in this regard, Dr Fitchett gave a letter about a patient, saying that she exhibited signs of paranoia, to her husband, whose lawyer produced it in open court during separation proceedings. The doctor was held liable for damages in respect of the nervous shock sustained by his patient because of his negligence. Thus, enforcement of the duty may lead to not only damages for the breach of confidence per se, but also liability for any consequential losses which might flow.

In certain circumstances breach of confidence may be justified, however, it may still be actionable if the disclosure goes further than that which is necessary. For example, the revelation that a woman is HIV positive may occasionally be justified. A doctor who, at the same time, points out that this was discovered during an abortion procedure will be in breach of confidence(Stauch et al., 2002). However, additional information may be revealed if it is necessary by way of explanation. In most states in Australia, legislation requires confidentiality on the part of healthcare practitioners employed by the State(*Health Administration Act* , 1982).

iii. In Griswold v. Connecticut(*Griswold v. Connecticut* , 1965), the Supreme Court held that the constitutional right to privacy, derived from the "*penumbras and emanations*" of the Bill of Rights, encompasses the right of married persons to use contraceptives. Justice Goldberg, in concurrence, relied extensively on the Ninth Amendment, which states that the specific rights enumerated in the Bill of Rights are not exhaustive.

iv. In the case of Eisenstadt(*Eisenstadt v. Baird*, 1972), the Court recognized that the right to privacy protects access to contraceptives for the married and unmarried alike. The opinion states, "*If the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child*."

v. The 1973 Supreme Court decision in Roe v. Wade(*Roe v. Wade*, 1973) was far from radical it was the logical extension of Supreme Court decisions on the right to privacy dating back to the turn of the century and used the same reasoning that guarantees our right to refuse medical treatment and the freedom to resist government search and seizure. In finding that the constitutional right to privacy encompasses a woman's right to choose whether to continue a pregnancy, the Supreme Court continued a long line of decisions that rejected government interference in life's most personal decisions.

vi. M.P. Sharma & Ors. vs. Satish Chandra and Ors. 1954(*M.P. Sharma & Ors. vs. Satish Chandra and Ors.*, 1954) was the first supreme court case where the matter related to privacy was discussed. The eight-judge bench of the court discussed the right to privacy and its interplay with Article 20(3). In this judgement, the court held that search and seizure of the documents did not amount to compelled testimony and in thus not violative Article 20 (3) and had relied upon decisions of the US Supreme Court interpreting the Fourth Amendment of the US Constitution. The Court rejected this argument as it observed that the Constitution of India did not have a fundamental right to privacy analogous to that of the Fourth Amendment of the US Constitution. The Court refused to import the principles of the Fourth Amendment in the form of the right to privacy.

vii. Kharak Singh vs. State of Uttar Pradesh and Ors. 1962(*Kharak Singh vs The State Of U. P. & Others* , 1962), the petitioner argued that all the clauses of Regulation 236 violated his constitutional freedom "*to move freely throughout the territory of India"* guaranteed under Article 19(1)(d) and "*personal liberty"* under Article 21. The court held that:

"*The right to personal liberty takes in not only a right to be free from restrictions placed on his movements, but also free from encroachments on his private life. It is true our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty. Every democratic country sanctifies domestic life; it is expected to give him rest, physical happiness, peace of mind and security. In the last resort, a person's house, where he lives with his family, is his "castle": it is his rampart against encroachment on his personal liberty.*"

viii. Govind vs. State of Madhya Pradesh & Ors 1975(*Govind vs State Of Madhya Pradesh & Anr* , 1975), in this case, three Judge Bench of the Supreme Court for the first time extensively discussed the right to privacy under Articles 19(1)(d) and 21 of the Constitution in the context of police surveillance. The writ petition challenged the validity of Regulations 855 and 856 of the Madhya Pradesh Police Regulations made by the Government under the Police Act, 1961 (Police Act) that permitted domiciliary visits and other forms of surveillance of individuals with criminal history. The Court held that even if it was assumed that the freedoms under Article 19 and Article 21 gave rise to a distinct fundamental right of privacy, this right could not be absolute and would be subject to restrictions based on the compelling public interest test as under Article 19(5). For this, the Court also relied on the example of Article 8 of the European Convention on Human Rights, which recognized the right to privacy but also allowed for reasonable restrictions on its enjoyment.

ix. R. Rajagopal & Ors. vs. State of Tamil Nadu & Ors. 1994(*R. Rajagopal vs State Of T.N*, 1994), was dealt with questions concerning the freedom of press vis-à-vis the right to privacy. The court held:

"*The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a "right to be let alone". A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, childbearing, and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages. Position may, however, be different, if a*

person voluntarily thrusts himself into controversy or voluntarily invites or raises a controversy."

x. Mr. X vs. Hospital Z 1998(*Mr. X vs. Hospital Z*, 1998), in this appeal on the grounds that disclosure of his HIV(+) status by the Respondent-Hospital was violative of medical ethics pertaining to confidentiality and also infringed upon his right to privacy under Article 21. The court held that:

"Right of Privacy may, apart from contract, also arise out of a particular specific relationship which may be commercial, matrimonial, or even political.... Doctor-patient relationship, though basically commercial, is, professionally, a matter of confidence and, therefore doctors are morally and ethically bound to maintain confidentiality. In such a situation, public disclosure of even true private facts may amount to an invasion of the Right of Privacy which may sometimes lead to the clash of [a] person's "right to be let alone" with another person's right to be informed."

xi. Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. 2017(*Justice K.S.Puttaswamy(Retd) vs Union Of India*, 2017), in this case began with the question of whether the right to privacy a fundamental right was, which was raised in 2015 in the arguments concerning the legal validity of the Aadhaar database. The case began with the question of whether the right to privacy a fundamental right was, which was raised in 2015 in the arguments concerning the legal validity of the Aadhaar database.

2.3.1. Privacy as discussed Internationally

i. Universal Declaration of Human Rights (UDHR), 1948

The UDHR was drafted in the years 1946-48. From the beginning, it was clear that privacy would be guaranteed in one form or another. It already contained a provision for the protection of privacy, even if not in a very prominent place. In Article 12, "*No one shall be subjected to arbitrary searches or seizures, or to unreasonable interference with his person, home, family relations, reputation, privacy, activities, or personal property. The secrecy of correspondence shall be respected*."

This is essential to the development of human personality and protection of human dignity, one of the main themes of the UDHR. It allows us to protect ourselves from unwarranted interference in our lives, and to determine how

we want to interact with the world and helps us to establish boundaries to limit who has access to our bodies, places, and things, as well as our communications and our information.

ii. Convention for the Protection of Human Rights and Fundamental Freedoms, 1950

Article 8 of the European Convention on Human Rights provides a right to respect for one's "*private and family life, his home and his correspondence*", subject to certain restrictions that are "*in accordance with law" and "necessary in a democratic society*". The European Convention on Human Rights (ECHR) (formally the Convention for the Protection of Human Rights and Fundamental Freedoms) is an international treaty to protect human rights and fundamental freedoms in Europe. Article 8 clearly provides a right to be free of unlawful searches, but the Supreme Court of US has given the protection for "*private and family life*" that this article provides a broad interpretation, taking for instance that prohibition of private consensual homosexual acts violates this article. This may be compared to the jurisprudence of the United States Supreme Court, which has also adopted a somewhat broad interpretation of the Right to Privacy.

iii. International Covenant on Civil and Political Rights (ICCPR), 1966

Article 17 is a short but versatile provision, capable of answering a broad diversity of unlawful or arbitrary incursions into privacy, home, family and correspondence, and unlawful attacks on reputation, including many instances which could not have been specifically foreseen by its drafters.18 years later since the adoption of the UDHR, privacy was recognized in Article 17 of the ICCPR using a similar language to Article 12 of the UDHR.

To illustrate the scope of Article 17, among in healthcare sector, it requires that the storage and use of personal information by the state (including telephone communications, correspondence, DNA and medical records) be confined and suitably safeguarded; it entitles anyone to know what personal data is officially stored about them and to be given the opportunity to correct it; it curbs defamatory statements, even in some circumstances the false attribution of authorship; it puts constraints on intrusive questioning of a rape victim about their sexual history; it protects the home against search, forced

entry and demolition, as well as the seizure of personal effects; it may be invoked to prevent the breakup of the family by deportation; it supports indicia of self-identity (such as one's name or gender); and it may be used to resist forcible medical procedures, as well as to secure access to certain medical procedures.

iv. OECD Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data, 1980s

Privacy protection laws have been introduced, in approximately one-half of OECD Member countries (Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States have passed legislation. Belgium, Iceland, the Netherlands, Spain, and Switzerland have prepared draft bills) to prevent what are violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data.

In Article 1(c), 3(a) and 5(b) of the OECD guidelines governing the protection of privacy in 1980s Convention recognizing:

- That, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information.
- That, automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices.
- That, transborder flows of personal data contribute to economic and social development.
- That domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows.

On the other side, OECD has been playing an important role in promoting respect for privacy as a fundamental value and a condition for the free flow of personal data across borders.

v.The Convention on the Rights of the Child (CRC), 1989

The Convention on the Rights of the Child, 1989 (CRC) is another important UN document that attempts to ensure, among others, a child's privacy interest

and to protect rights. The Convention explains who children are, all their rights, and the responsibilities of governments. All the rights are connected, they are all equally important and they cannot be taken away from children.

Article 16 of the convention on the rights of the child, 1989 affirms that "*No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, or correspondence, nor to unlawful attacks on his or her honour and reputation. The child has the right to the protection of the law against such interference or attacks*."

vi. The International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, 1990

The next UN initiative was the adoption of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, 1990, which aims to protect various rights of migrant workers and their family members, including privacy.

Article 14 of the International Convention on the protection of the rights of all migrant workers and members of their families, 1990. States that "*No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, correspondence or other communications, or unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks."*

vii. The Special Rapporteur on the Right to Privacy, 2015

Privacy enables the enjoyment of other rights: the free development and expression of an individual's personality, identity and beliefs, and their ability to participate in political, economic, social, and cultural life. The UN efforts and promises for the protection of privacy have also been manifestly apparent through the Reports of the UN Special Rapporteur on the Right to Privacy. In July 2015, the UN Human Rights Council appointed Professor Joseph A. Cannataci as its first-ever Special Rapporteur to work on the project 'The Right to Privacy in the Digital Age'.

<u>The Special Rapporteur is mandated to promote and protect the right to privacy by:</u>

- Reviewing government policies and laws on the interception of digital communications and collection of personal data
- Identifying actions that intrude on privacy without compelling justification.
- Assisting governments in developing best practices to bring global surveillance under the rule of law.
- Articulating private sector responsibilities to respect Human Rights.
- Helping ensure national procedures and laws are consistent with International Human Rights obligations.

2.3.2. Privacy across multiple disciplines

Almost all authors on privacy start the discussion with the famous article '*The Right to Privacy* by Samuel Warren and Louis Brandeis in the Harvard Law Review of December 15, 1890. Although the effects of this research cannot be underestimated this starting point does not mean that there have been no discussions on the invasions of privacy before 1890. As Westin shows in his publications, in the fifteenth century, the word '*privacy*' was already used in England and historical research shows that colonists in New England were respecting privacy in relation to an individual's home, family, and even written communication. Hixson shows that there was opposition against the first U.S. census as early as 1790, although the government required little more than the enumeration of persons, both slave and free. This opposition resulted in instructions to census takers in 1840 that individual returns be treated as confidential. It was feared that the citizen was not adequately protected from the danger that private affairs or the secrets of the family would be disclosed to the neighbors. Privacy can be understood in it connect perspective through the following:

i. Trespass

Privacy is a concept intricately relating to trespassing. We have numerous instances decided by different courts both nationally and internationally. To gauze the true nature of the term privacy a quick look into this interpretation is called for.

British Lord Camden, striking down a warrant to enter a house and seize papers wrote '*We can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society, for papers are often the dearest property any man can have*'. The law of trespass and the constitutional protection of unreasonable search and seizure in the United States as formulated in the Fourth Amendment were interpreted as protections against official and unofficial intrusions.

ii. **Correspondence**

Long before this protection was generally accepted, in particular using the telegraph, the first incidents about invasion of reading personal mails are known. Plymouth Plantation was the scene for what Hixson mentions as the first recorded invasion of privacy. Governor William Bradford learned of a plot against the leadership of the small colony. He had intercepted several incriminating letters written by two newcomers and sent to friends in England. When the two men denied any conspiracy, the governor produced the letters and asked them to read the content aloud. The men expressed outrage that their private correspondence had been intercepted but did not comply further since they had no legality on which to stand.

iii. **The Press**

Curiosity has always been an enemy of privacy and is a foible that has stimulated privacy invasion and on which newspapers have exploited individual privacy on a commercial basis. Already in 1873, the first complaints were made against the way journalists were using interview techniques. President Cleveland expressed dislike of the way the press treated him on occasion, especially when some journalists followed him and his bride on their honeymoon trip in 1886. Also, E.L. Godkin wrote at the end of the 19th century that the chief enemy of privacy in modern life is the curiosity shown by some people about the affairs of other people. Although it is not known how far Warren and Brandeis were influenced by Godkin, generally the discussion on the attack on privacy starts with the famous article of these two lawyers, published in 1890 in the Harvard Law Review under the title '*The Right to Privacy'*. The reason for publication grew out of a specific

situation. The Saturday Evening Gazette, which specialized in '*blue blood items*' reported activities of Warren and his wife in lurid details. Warren, together with Louis D. Brandeis, was the first to start a fundamental discussion on his right not to have his thoughts, statements, or emotions made public without his consent. Since the publication of this famous article, no contribution to the issue of privacy fails to mention it.

iv. Instantaneous Photography

In one of the researches, Warren and Brandeis not only blame the press but also recent inventions and business methods like instantaneous photographs. In combination with the newspaper business, these business methods and new technologies invaded sacred personal and domestic precincts. As predicted in the famous Warren and Brandeis article, these numerous mechanical devices would be the source for what is whispered in the closet shall be proclaimed from the housetops. A classic type of invasion of privacy is the use without consent of a person's picture to promote a product. The initial test was Roberson v. Rochester Folding Box Co., which startled the New York legal world. A local milling company decided to use a photo of Abigail Rochester, a charming and attractive girl at the time, to promote their product. For that reason, the brilliant slogan The Flour of the Family was used and, together with the photo, placed in numerous stores, warehouses, and saloons. Abigail claimed the '*Right of Privacy'* and sued for the sum of $15,000. The New York Court denied the suit, by a 4-3 decision, saying that her claim held no right on grounds that it was yet unknown to common law what had been infringed.

V. Medical Records in healthcare

Medical record is a document pertaining to a patient's medical history, diagnoses and therapies, and status when last seen by healthcare providers. It also includes some of the most intimate details about a person's life. The document consists of a patient's physical and mental health and can include information on social behaviors, personal relationships, and financial status.

2.4. Privacy in the Context of Healthcare

The medical community has long recognized the importance of protecting privacy in maintaining public trust in doctors and researchers, and codes of

medical ethics reflect a desire to increase this public trust. Since the time of Hippocrates, physicians have pledged to keep information about their patients private and confidential. The Hippocratic Oath states, "*What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself….".* This pledge to privacy has been included in the code of ethics of nearly all health care professionals in the United States. For example, the first Code of Ethics of the American Medical Association in 1847 included the concept of confidentiality.

The value of health information privacy has also been recognized by affording it protection under the law (reviewed by Pritts). The rules for protecting the privacy of health information in the clinical care and health research contexts developed along distinct paths until the promulgation of the federal privacy regulations under HIPAA. Prior to HIPAA, health information in the clinical setting was protected primarily under a combination of federal and state constitutional law, as well as state common law and statutory protections.

The doctor-patient relationship is based upon trust. For proper diagnosis and treatment, it is essential that during treatment a patient discloses truthfully to the physician about his illness. Patients are required to share information sometimes utmost personal with their physicians to facilitate correct diagnosis and treatment to avoid adverse drug prescriptions and further complications in their physical health. This may sometimes involve disclosure of personal and sensitive information to the doctors. A patient expects that the private information disclosed to a doctor will remain confidential. Also, a right-based approach might regard the duty of keeping confidences as a respect for the right to privacy.

The doctor consulting room should be as sacrosanct as the priest confessional. The whole of the art and science of medicine is based on the intimate personal relationship between patient and doctor, and to this it always returns, however scientific medication become and whatever the great and undeniable benefits society receives from the application of social and preventive medicine.

Further both deontological and teleological reasoning can be used to justify the existence of a duty of confidence between patients and doctors. The

consequentiality argues that optimum medical care and protection can be provided to patient of a doctor is able to provide a scene of emotional and personal assurance that his midscale information will not be disclosed so that a patient never finds himself in an embarrassing position while talking to the physician about his illness. Doctors routinely ask a series of questions about bodily functions that people would not dream of discussing with anyone else. As Raanan Gillon also discussed:

'*When a patient's medical problem may relate to genitourinary functions a doctor may need to know about that patient's sexual activities, sometimes in detail. When patient problems are psychological a doctor may need to know in great details about the patient's* experiences ideas and feedings relationship past and present even in some contexts the person imaginings and fantasies.'

Such intensive medical inquiries are based not on prurience or mere inquisitiveness but on the pursuit are based not on prurience or mere inquisitiveness but on the pursuit of information that is of potential assistance to the doctor in treating and helping the patient. Nonetheless many patients are unlikely to pass in this information unless they have some assurances of confidentiality.

Hence according to consequentiality justification for the duty of medical confidentiality is people better health, welfare, the general good and overall happiness. The language of the public interest defense has a strong utilitarian flavor. The utilitarian view is particularly appropriate to confidentiality as it will readily admit that the duty is not absolute and can be breached in certain circumstances. It would be argued that the breach is justified when the utility of disclosure outweighs the utility produced by keeping the confidences. As will be seen, the only legal justification at common law for disclosure is either that the patient had consented or that it is in the public interest to disclose. According to deontological theorists, it is the duty rather than purpose which is the fundamental concept of ethics. At the end both utilitarians and paleontologists alike as means to some morally desirable end calls for the general welfare, respect for people autonomy and respect for their privacy.

Confidentiality is beneficial for individual patients and for the community at large. For example, in the context of transmittable diseases, especially

sexually transmittable diseases so long as the patient continues to trust his or her doctor, the doctor will be able to educate and influence the patient in ways that can reduce the likelihood of the disease being passed on to other member of the community. As soon as confidentiality is broken the trusting relationship is likely to be undermined and the opportunity to help reduce the spread of disease is lost. On the other hand, if a patient confides in his doctor that he has committed a very serious crime such as child abuse should the doctor inform the police or keep the information confidential and similarly in the case of drug use? Here no one will deny that there is a clear public interest for pedophiles and drug users to willingly come forward to seek help. Thus, Emily Jackson strongly argues that working out whether disclosure is justified in a particular case will often involve a completed balancing exercise between competing interests.

Doctors in India since Vedic times have been equated to God. That is one of the reasons that the profession of a doctor is the most pious, noble and respected. The ability of a doctor to cure the patients commands immense trust in his patients. It is, therefore, imperative for a doctor that he must not let down his patients and give his patients all due care and attention. Needless to emphasis that any negligence on the part of a doctor may cause severe hardships for the patient, even leading to his death.

The duty to maintain confidentiality has its origin in the Hippocratic Oath, which is an ethical code attributed to the ancient Greek physician Hippocrates, adopted as a guide to conduct by the medical profession throughout the ages and still used in the graduation ceremonies of many medical schools and colleges: Hippocrates lived and practiced as a Physician between third and first Century B.C. He has been referred to by Plato as a famous Ascleplad who had a philosophical approach to medicine. In his manuscripts, the Hippocratic Collection (Corpus Hippocracticum), contained the Hippocractie Oath.

The Oath consists of two parts. The first, or covenant; is the solemn agreement concerning the relationship of apprentice to teacher and the obligations enjoined on the pupil. The second part constitutes the ethical code.

It is based on the above that International Code of Medical Ethics has laid down as under:

'*A physician shall preserve absolute confidentiality on all he knows about his patient even after his patient has died*.'

In India, there is the Indian Medical Council Act, which controls the medical education and regulates the professional conduct. Section 20A which was inserted by the Indian Medical Council (Amendment) Act 1964 provides as under:

- **Professional Conduct**

  The Council may prescribe the standards of professional conduct and etiquette and a code of ethics for medical practitioners, (2) Regulations made by the Council under sub-Section (1) may specify which violations thereof shall constitute infamous conduct in any professional respect, that it is to say, professional misconduct, and such provision shall have effect notwithstanding anything Contained in any law for the time being in force.

  Medical information about a person is protected by the Code of Professional Conduct made by the Medical Council of India under Section 33(m) read with Section 20A of the Act. The relevant provisions of the Code of Medical Ethics have already been reproduced above which contain an exception to the general rule of confidentiality, in as much as it provides that the information may be disclosed in a court of law under the orders of the Presiding Judge. This is also the law in England where it is provided that the exceptions; to this rule permit: disclosure with the consent, or in the best interests, of the patient, in compliance with a court order or other legally enforceable duty and, in very limited circumstances, where the public interest so requires. Circumstances in which the public interest would override the duty of confidentiality could, for example, be the investigation and prosecution of serious crime or where there is an immediate or future (but not a past and remote) health risk to others.

  The Code of Medical Ethics also carves out an exception to the rule of confidentiality and permits disclosure. In the circumstances enumerated above under which public interest would override.

  The right to privacy has been culled out of the provisions of Article 21 arid other provisions of the Constitution relating to Fundamental Rights read with Directive Principles of State Policy. It was in this context that it was held by the Court in Kharak Singh v. State of Uttar Pradesh, that police surveillance

of a person by domiciliary visits would be violation of Article 21 of the Constitution, this decision was considered by Mathew, J. in his classic judgment in Govind v. State of Madhya Pradesh & Anr. in which the origin of "right to privacy" was traced and several American decisions, including Munn v. Illinois, Wolf v. Colorado, and various types of research were considered arid it was laid down ultimately, as under:

"*Depending on the character and antecedents of the person subjected to surveillance as also the objects and the limitation under which surveillance is made, it cannot be said surveillance by domiciliary visits would always be unreasonable restriction upon the right of privacy. If the fundamental rights explicitly guaranteed to a citizen have penumbral zones and that the right to privacy is itself a fundamental right that fundamental right must be subject to restriction based on compelling public interest."*

As one of the basic Human Rights, the right of privacy is not treated as absolute and is subject to such action as may be lawfully taken for the prevention of Crime or disorder or protection of health or morals or protection of rights and freedoms of others.

The right of Privacy may, apart from contract, also arise out of a particular specific relationship which may be commercial, matrimonial, or even political. As already discussed above, Doctor-patient relationship, though basically commercial, is, professionally, a matter of confidence: and there-fore, Doctors are morally and ethically bound to maintain confidentiality. In such a situation, public disclosure of even true private facts may amount to an invasion of the Right of Privacy which may sometimes lead to the clash of one person '*Right to be let Alone'* with another person right to be informed. Disclosure of even true private facts has the tenancy to disturb a person's tranquility.

In the face of these potentialities and as already held by this Court in its various decisions referred to above, the Right of Privacy is an essential component of right to life envisaged by Article 21, The right, however, is not absolute and may be lawfully restricted for the prevention of crime, disorder or protection of health or morals or protection of rights and freedom of others.

- **Ethical Obligation**

A doctor's duty to respect his or her patient's confidentiality has its origin in the first code of medical ethics. Oath of Hippocrates are:

'*What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself holding such things shameful to be spoken about*.'

In India, the above undertaking is respected in the Indian Medical Council (Professional Conduct Etiquette and Ethics) Regulation 2002. The Medical Council of India's Code of Ethics Regulations protects patient confidentiality by stating that the physician shall not disclose the secrets of patient that have been learnt in the exercise of his or her profession except in a court of law under orders of the Presiding Judge in circumstances where there is a serious and identified risk to a specific person and or community or in case of notifiable diseases. In addition to treating doctors, administrators and the public information officer of a health care institution are also ethically requited not to disclose hearth information of a patient. Similarly, according to Indian Council of Medical Research (ICMR) guidelines for biomedical research on human participants, researchers must maintain the confidentiality of their subject's health and other personal information, especially as the promise of preserving confidentiality is appropriately part of the informed consent agreement.

In case of Spy catcher case, Lord Goff said that "*A duty of confidence arises when confidential information comes to the knowledge of a person...in circumstances where he has notice or is held tot have agreed that the information is confidential with the effect that it would be just in all the circumstances that he should be precluded from disclosing the information to others*."

Lord Woolf stated that a duty of confidence will arise whenever the party subject to the duty is in a situation where he either knows or ought to know that the other person can reasonably expect his privacy to be protected. It is both the nature of the information and the circumstances in which it was disclosed that create the duty of confidentiality.

The nature of this obligation which applies to all confidential information and not only to medicine was discussed by the Court of Appeal in A-G v. Guardian Newspapers Ltd also known as Spy catcher case in which it was affirmed that there was a public interest in a legally enforceable protection of confidence received under notice of confidentiality. Moreover, the obligation may be imposed by an express or implied term of contract or can even exist independently of any contract based on an independent equitable principle of confidence. In Ashworth Security Hospital v. MGN Ltd, Lord Phillips MR held that there is an inherent obligation of confidentiality between doctor and patient and when a patient enters a hospital for treatment whether he be a model citizen or murderer he is entitled to be confident that details about his condition and treatment remain between himself and those who treat him.

To determine whether the circumstance of communication is confidential, McInerney J, in Menes v. Mikenkovic expressed that there must be an objective test. This approach was clearly expressed in following words:

"If the circumstance is such that any reasonable man standing in the shoes of the recipient of the information would have realized that upon reasonable grounds the information was being given to him in confidence, then this should suffice to impose on him the equitable obligation of confidence."

Therefore, equity may impose an obligation of confidence upon a defendant having regard to not only what the defendant knew but to what he ought to have known in all the relevant circumstances. In other words, even if the revelation did not itself harm a particular person, if it could be said to have caused public harm, for example to lead to a lack of trust in doctors, this could be sufficient to justify protecting the information in equity.

2.4.1. The significance and necessity of Patient-Privacy-Protection

Protecting the security of data in health research is important because health research requires the collection, storage, and use of large amounts of personally identifiable health information, much of which may be sensitive and potentially embarrassing. If security is breached, the individuals whose health information was inappropriately accessed face a few potential harms. The disclosure of personal information may cause intrinsic harm simply because that private information is known by others. Another potential danger

is economic harm. Individuals could lose their job, health insurance, or housing if the wrong type of information becomes public knowledge. Individuals could also experience social or psychological harm. For example, the disclosure that an individual is infected with HIV, or another type of sexually transmitted infection can cause social isolation and/or other psychologically harmful results. Finally, security breaches could put individuals in danger of identity theft.

Protecting the privacy of research participants and maintaining the confidentiality of their data have always been paramount in research and a fundamental tenet of clinical research. However, several highly publicized examples of stolen or misplaced computers containing health data have heightened the public concerns about the security of health data. The extent to which these breaches have caused tangible harm to the individuals involved is difficult to quantify. A Government Accountability Office (GAO) report studying major security breaches involving nonmedical personal information concluded that most security breaches do not result in identity theft. However, the lack of identity theft resulting from past breaches is no guarantee that future breaches will not result in more serious harm. A recent report from the Identity Theft Resources Center found that identity theft is up by 69 percent for the first half of 2008, compared to the same time in 2007. Also, regardless of actual harm, security breaches are problematic for health research because they undermine public trust, which is essential for patients to be willing to participate in research. A recent study found patients believe that requiring researchers to have security plans encourages researchers to take additional precautions to protect data. Moreover, data security is important to protect because it is a key component of comprehensive privacy practices.

2.4.1.1. Human Rights in relation to privacy and healthcare

The unauthorized disclosure of medical information is a human rights issue and has been clearly established by the European Court of Human Rights. The European Convention on Human Rights incorporated into English law by the Human Rights Act 1998 protects right to a private life under Article 8. This Article impliedly protects patient interest in privacy and medical confidentiality apart from the right to respect for private and family life.

Article 8(2) makes it clear that rights can be limited provided they are prescribed by the law and are necessary in a democratic society for several specified aims including the right and freedom of others the prevention of crime and the protection of health and morals. It is clear however that a broad range of privacy interests are encompassed within Article 8 protection including an individual's relations with others physical and moral integrity, personal integrity legal recognition of gender and sexuality as well as the more obvious aspects of personal information. It is difficult for individuals to establish that any disclosure of their medical records constitutes a prima facie violation of Article 8. The principal obstacle to a successful claim is that it has been possible for public authorities to establish that disclosure is justifiable under Article 8(2). In MS v. Sweden, the applicants claim for industrial injury compensation led to her medical record, including sensitive information about termination of pregnancy being forwarded to the social insurance office without her knowledge. The European Court confirmed that disclosure of confidential information as an interference with the applicants Article 8 (1) rights, but it was justified under Article 8(2) on the grounds of protecting the economic wellbeing of the country because the medical information was relevant to the granting of public funds.

In Z v. Finland, for example Z was married to someone who had been charged with several sexual offenses. He was HIV positive and to find out when he became aware of his HIV states the police sought and gained access to Z's medical records. The ECHR held that seizing Z's medical and ordering her doctors to give evidence did not amount to a violation of Article 8 because although a patient has an important interest in protecting the confidentiality of his or her medical records that interest may be outweighed by the Government's interest in investigating and persecuting a crime. However, the European Court of Human Rights stated:

"*The protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by article 8 of the convention without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be*

necessary in order to receive appropriate treatment and, even, from seeking such assistance, there by engendering their own health and in the case of transmissible disease, that of the community."

Autonomy is the underlying concept of modern human rights law and therefore privacy occupies a central role in ensuring that individual have the freedom from state interference to give their other rights like right like right to life, dignity, liberty, freedom of expression and religion etc. a meaning. It is this aspect which is of vital significance to medical confidentiality. Before discussing medical confidentiality, it is also necessary to understand the difference between the right to privacy and the right to have confidential information protected. The law imposes several requirements in order for a cause of action to arise for breach of confidence, and these criteria mean that for example press photographers own no duty of confidence unless the photography takes place in confidential circumstances or there had been a prior agreement not to publish. If neither of these applies, only a right to privacy can offer protection from publication. In another example a private diary dropped in a public place and found by a passerby would be protected by a duty of confidence. This has led some commentators to argue that the rationale has moved from the protection of confidence to the protection of privacy and that any distinction between a duty of confidence and a tort of privacy has vanished.

2.5. Conclusion

The concept of privacy has a deep historical background, with its roots dating back to ancient civilizations where individuals actively sought solitude and seclusion. Even in the communal living arrangements that were common in early societies, individuals were aware of the significance of establishing personal boundaries and zones. In the ancient Roman period, individuals of high social standing maintained private chambers within their homes, emphasizing the importance placed on personal spatial boundaries and the safeguarding of confidential affairs. The notion of privacy became progressively intertwined with cultural, religious, and legal structures as societies underwent transformation. During the Enlightenment era, the

examination of individual rights and the extent to which government should intervene garnered considerable interest. This was notably explored by influential thinkers like John Locke and Jeremy Bentham. The notion of safeguarding against unwarranted intervention has since been established as a fundamental principle in various legal systems across the globe. The preservation of privacy is of great importance and plays a crucial role in safeguarding the fundamental rights and dignity of individuals within a particular society. Privacy serves as a safeguard against illegal intrusion into personal matters, empowering individuals to retain authority and autonomy over their own existence. Establishing trust between individuals and institutions, regardless of whether they are governmental, business, or social in nature, is an essential element. The maintenance of the freedom of speech relies on the protection of privacy, as individuals are more likely to engage in unrestricted self-expression when they have a sense of safety within their personal spheres. Moreover, the notion of privacy assumes a vital role in shaping one's own identity and fostering intimate social relationships. The lack of assurance over privacy can potentially lead individuals to exhibit hesitancy in participating in self-reflection and genuine self-disclosure, so hindering personal growth and societal progress.

This chapter explores the historical development of the notion of privacy and highlights the enduring significance placed on privacy since ancient times. The notion of privacy has been deliberated in numerous domestic and international legal decisions. In these instances, this discussion will elucidate the significance of privacy within several domains, such as the confidentiality of personal correspondence, the privacy within familial and relational contexts (e.g., married life), the protection of children's privacy, the confidentiality of telephonic conversations, and the safeguarding of medical records pertaining to patients within the healthcare sector. The focal focus of the present chapter pertains to the subject of privacy within the healthcare domain, emphasizing the paramount significance of safeguarding patient confidentiality. The next part elucidates the evolving trajectory of patient privacy in relation to the increasing prominence of patient data considering technological advancements. The progression of technology within the

healthcare sector has resulted in a transformation of conventional practices and diagnostic approaches employed within the healthcare system.

CHAPTER 3

DATA PROTECTION IN THE HEALTHCARE SECTOR: A GLOBAL SCENARIO

3.1. Introduction

Many novel digital technologies related to medicine and health look poised to transform medical practices and challenge traditional conceptions of the doctor-patient relationship(Boeldt et al., 2015). Several recent research has investigated the moral repercussions of this, probing, for instance, whether "greater efficiency, consistency, and reliability might do so at the expense of meaningful human interaction in the care context" when using innovative approaches(Topol et al., 2015). The rapid adoption of new tools, techniques, and different machines has been observed to have a significant impact on the socioeconomic structure of society. This results in less manual work and aids in ubiquitously interconnecting everyone with the help of the Internet of Things (IoT), which offers smooth and seamless services for everyone(Apthorpe et al., 2017). IoT refers to the networking of physical devices that are smart, and interconnected(Thilakarathne et al., 2020), comprising sensors, software, and network connectivity that enables them to collect and exchange data(Alsubaei et al., 2017). When it comes to technology in the healthcare sector, it refers to a wide variety of smart devices whose main purpose is to facilitate and aid in fundamental patient care(Pirbhulal et al., 2019). As of now, healthcare providers are utilizing various IoT, Artificial Intelligence(AI)(*What Is Artificial Intelligence and How Is It Used?*, 2020), and Blockchain-based technology in the applications and services for patient treatment, disease management, and medical diagnosis, to improve patient care and lower the costs of care(Alsubaei et al., 2017).

These devices or the new technology collect various patient sensitive data such as vital body parameters and monitor pathological details by implantable medical sensors or small wearable sensors that are worn by the patient(Alsubaei et al., 2019; Pirbhulal et al., 2019). Currently, the market for advanced technology in healthcare services has increased exponentially. At the same time, security issues in the system also increase this situation threatening the privacy and protection of the patient's sensitive data(Somasundaram & Thirugnanam, 2021). Smart devices and applications used in the healthcare sector are prone to severe security vulnerability.

In this chapter, there will be a quick overview of the healthcare system and how privacy concerns are gradually shifting to focus on patient health data. The dramatic shift that the introduction of new technologies has brought about in the status quo of the healthcare sector. Explaining the role that AI and IoT-based devices play important role in improving the current healthcare system. The author also discusses the emerging challenges in the healthcare industry. What are the legal challenges that the healthcare sector faces, after the implementation of the new technologies or the IoT application? When it comes to the inter section of technology and law, why is it so crucial that there is a need to secure patient-sensitive data?

3.1.1. The Healthcare Industry

According to WHO(World Health Organization, 2019), '*the healthcare sector consists of individuals and organizations that provide health services but are neither owned nor directly regulated by the government. It can be divided into for-profit and non-profit, formal, and informal, domestic, and international subcategories*.'

India Brand Equity Foundation explained healthcare as, '*Healthcare comprises hospitals, medical devices, clinical trials, outsourcing, telemedicine, medical tourism, health insurance and medical equipment. The Indian healthcare sector is growing at a brisk pace due to its strengthening coverage, services, and increasing expenditure by public as well as private player.'*

In Occupational Safety and Health Administration(R joshi & M Parilh, n.d.) describe healthcare as, '*Healthcare is involved, directly or indirectly, with the provision of health services to individuals. These services can occur in a variety of work settings, including hospitals, clinics, dental offices, out-patient surgery centers, birthing centers, emergency medical care, home healthcare, and nursing homes*.'

In the healthcare industry, a variety of service delivery entities operate. Figure 3.1(*The Private Sector | Health Systems Global*, n.d.) depicts the subsectors of the healthcare field that operate within the health sector.

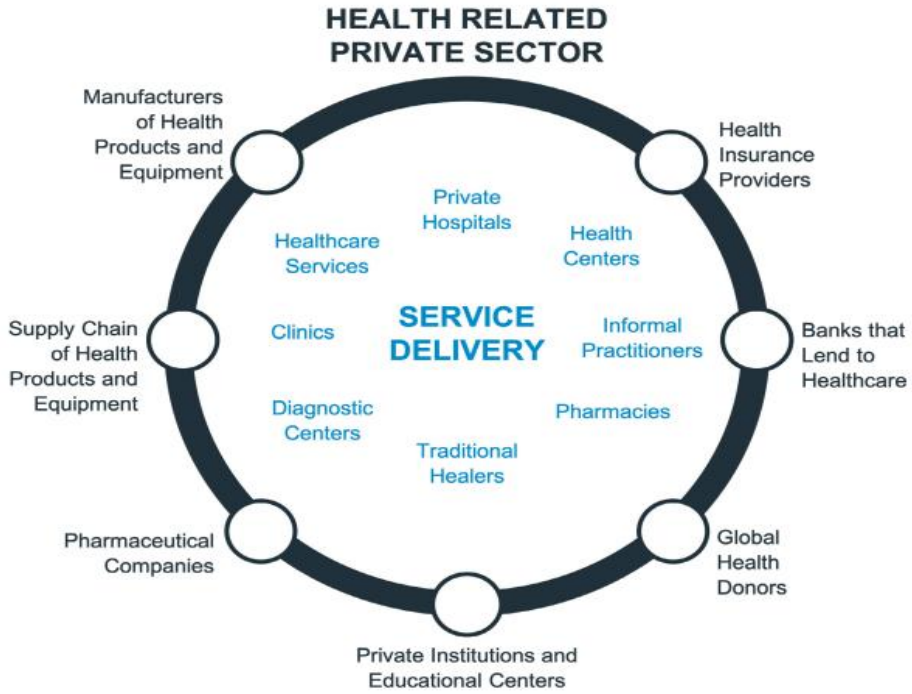

Figure 3.1 Different entities in the healthcare sector.

i. **Manufactures of health products and equipment**: Instruments, devices, and equipment intended for treatments, monitoring, and diagnostics comprise the medical device industry. There are also implantable devices for cardiac and diabetes care(*What Is Medical Manufacturing?*, n.d.).

ii. **Supply-chain of health products and equipment:** The healthcare supply chain, also known as Healthcare Supply Chain Management (SCM), covers the conveyance of medical equipment and legal drugs from producers to healthcare institutions. Financially and logistically efficient procurement and distribution of medical supplies and services from a manufacturer to a patient constitutes healthcare SCM. The major objective of establishing a supply

chain is to rapidly provide the necessary medical supplies to institutions such as hospitals, clinics, and pharmacies. One would be tempted to believe that the Healthcare SCM consists solely of placing an order for a list of medical equipment, such as medications, protective gear, and other medical supplies. However, this supply chain goes beyond this and focuses on acquiring the best resources for the patients at the chain's conclusion(*Healthcare Supply Chain*, n.d.).

iii. **Pharmaceutical companies**: Pharmaceutical Company refers to a manufacturer, seller, or distributor of pharmaceuticals, medications, or prescription drugs. The term "pharmaceutical firm" does not include a pharmaceutical benefits manager as defined in sub-section (c) or a health care provider(*Pharmaceutical Company Definition | Law Insider*, n.d.).

iv. **Private institutions and educational centers**: There has been an increase in the acknowledgment and recognition of the role that the private sector has played in the establishment of improved health systems and the advancement of healthcare all over the world.

v. **Global health donor**: Donating and transplanting a wide variety of organs and tissues is possible. Donating an organ benefit both the donor and the recipient. The impact on the family and friends of those who need a transplant is even greater than that on the donors and recipients themselves. The donor's loved ones can also benefit greatly from organ donation. Having the knowledge that their loved one is saving the lives of others can help a family cope with their loss and move through the grief process(*World Health Donors* , n.d.).

vi. **Bank that lends to healthcare**: As part of the proactive measures to mitigate the economic impact of an epidemic or emergency, the banking sector has developed a scheme of on-lending intervention for the healthcare sector. The goal of the initiative is to help local pharmaceutical firms and other organisations throughout the healthcare value chain expand their operations to fulfil the rising demand for medical services caused by the ongoing coronavirus pandemic(*Healthcare Sector Loan*, n.d.).

vii. **Health Insurance Provider**: In exchange for a premium, health insurance will pay for the insured person's medical care in the event of an illness or

injury. It allows the insurance company to pay for medical care such as hospitalisation, day care, severe sickness, etc. A health plan provides a variety of advantages, such as free preventative care and cashless hospitalisation(*Health Insurance*, n.d.).

viii. **Pharmacies**: Pharmacists play a crucial role in patient care by providing guidance on medication use and informing them of possible adverse reactions and drug interactions. They tell patients what to expect if they take the drug and what to do if they have any negative responses to it. In addition, pharmacists help patients get the most out of their drugs by identifying any factors that may be preventing them from taking their medications as prescribed(*Pharmacists and the Role They Play in Healthcare | United MSD Foundation*, n.d.).

ix. **Diagnostic centre**: Modern medicine relies heavily on the findings of diagnostic centres and laboratories. Diagnostic tests of high quality are crucial to the successful management of infectious illnesses. The potential for long-term consequences can be mitigated with prompt identification and treatment. A diagnostic centre is a medical facility that provides medical diagnostics to individuals of all ages and sexes(*Importance Of Diagnostic Centre – PDC Health*, n.d.).

x. **Private hospital**: Health care privatisation is the practice of contracting out the delivery of medical care and related services to for-profit businesses. Direct private sector involvement can include clinics, pharmacies, and hospitals; indirect private sector involvement might include suppliers of equipment and supplies(*Privatization in Health Care Services !! - Public Health Notes*, n.d.).

Additionally, the healthcare industry is described as the industry that delivers goods and services to treat patients with curative, preventative, rehabilitative, and palliative care(*What Is Health Sector* , n.d.).

Health care is the sum of preventive services and measures provided by the Directorate of Basic Health Care and its affiliated institutions to all members of society to enhance the overall well-being of the community and prevent the disease from spreading. This includes the provision of services that help to improve the general health level. Keep the environment and water free from

contamination. Caring for mothers during pregnancy and childbirth, as well as ensuring that children are properly fed and vaccinated on the plan. In the next paragraphs, the researcher will detail the two scenarios. The first is healthcare in its traditional form, while the second is healthcare in its technologically enhanced form.

3.2. Healthcare sector before technological era

Health institutions aim to provide a healthy environment for all members of the community, educate individuals healthily, control communicable diseases, and provide health, medical and nursing services to the community with early diagnosis. Globally, every nation is working and developing its healthcare sector. The healthcare industry can be divided into four primary components. The availability of hospitals comes first, followed by the expertise of medical professionals, and finally by the diagnostic and surgical equipment at their availability. Finally, we come to how patient information is stored. The continual availability of hospital services for acute and complex diseases complements and enhances the efficacy of many other aspects of the health system. As a result, they can more effectively address the healthcare requirements of their communities by focusing limited resources within carefully mapped-out referral networks. As such, they are crucial to achieving the Sustainable Development Goal of "Universal Health Coverage"(UHC)(*Hospital*, 2022).

The United States has 1,100,101 physicians in total as of January 2024 (figure 3.2). At over 119 thousand active doctors, California led the state in this regard, followed by New York. Conversely, Wyoming has the lowest active physician population in the country, just 1,245. More medical personnel are needed to keep up with the increasing demand and massive population. However, the data analysis shows that the United States will have a severe physician shortage. Intense action from the government is needed to remedy the situation, as is a shift toward smart technology that can help doctors with their daily tasks.

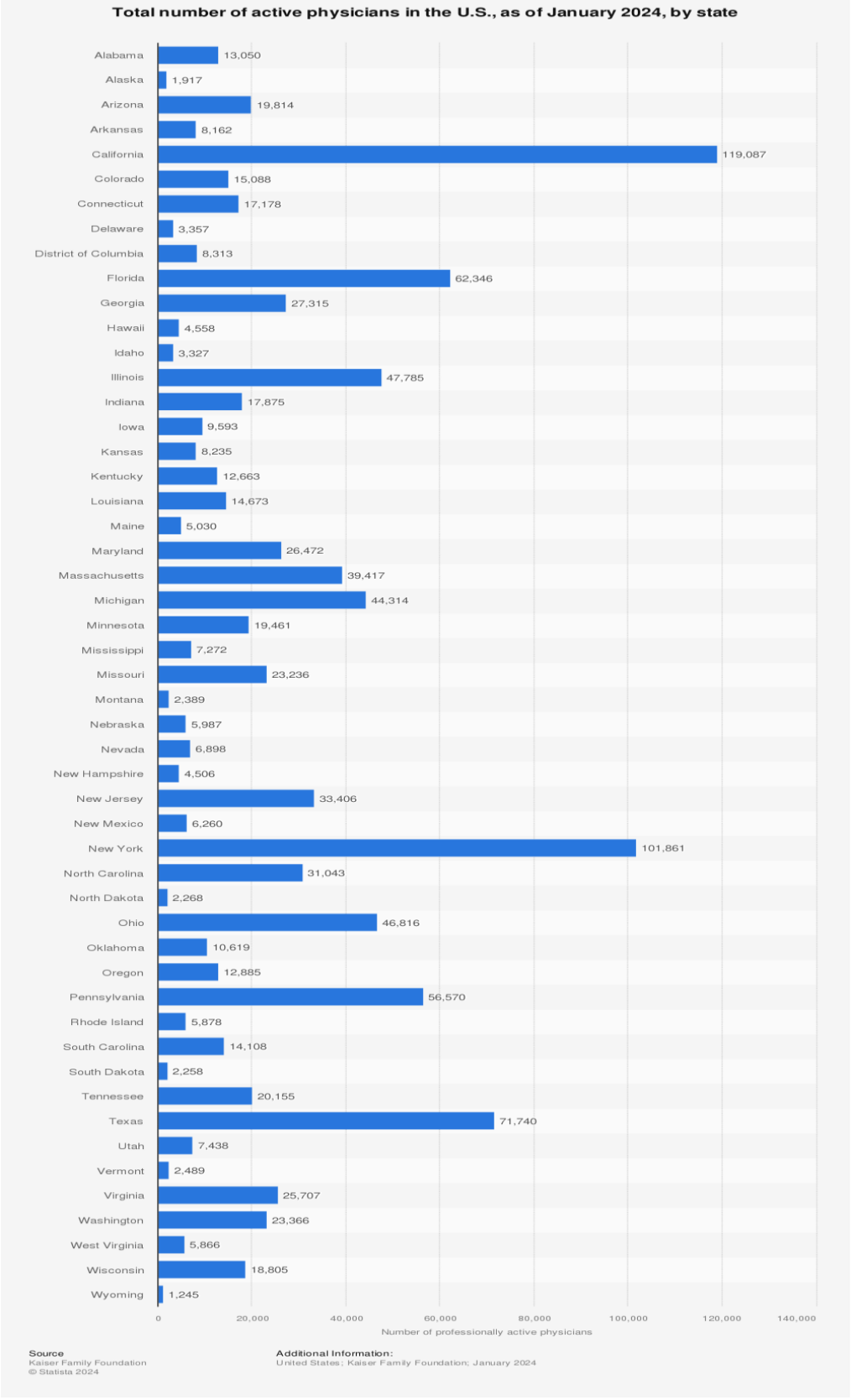

Figure 3.1 Number of active physicians in US, 2024(yang, 2024)

One of India's most important and rapidly expanding industries is healthcare. Hospitals, medical professionals, support staff, laboratory personnel, surgical and diagnostic tools, and a database of patient records all make up the healthcare system. The public and private sectors in India are investing more money and expanding their reach in the healthcare system, leading to rapid expansion(*Indian Healthcare Industry Analysis | IBEF*, 2022). Currently, India has a population of 1,421,673,905(*India Population* , 2023), making it the world's most populous democracy and number one globally. It is assumed that India has a robust healthcare system that adequately serves its citizens. An overview of the healthcare system is required for comprehension.

The number of hospitals including private and public, there are total 69,264 number of hospitals in India. With contrast to the population size, the figures are quite low in number and reflected in a rather poor prognosis for the health system.

Primary Health Services (PHCs) are not present in many villages (there is about 1 for every 20 villages), and where present are acutely undermanned. Moreover, as many as 18% of PHCs are entirely without doctors. The only redeeming feature of the system is the committed cadre of Auxiliary Nurse Midwifes (ANMs) who work at PHCs, and the accredited social health activists (ASHAs)(*Why India's Healthcare System Continues to Lag behind | Qrius*, n.d.).

This is true that Indian healthcare facilities have grown significantly in terms of numbers and the expertise of health professionals, but this growth has largely been confined to the private sector. It is the government's failure to deliver quality care that has led to the rapid expansion of private hospitals, which today account for 93% of all hospitals (up from 8% in 1947), 64% of all beds, and 80-85% of all doctors. However, affordability in Tier 3 cities and rural areas is a critical limiting factor for the further expansion of the private health sector(*Why India's Healthcare System Continues to Lag behind | Qrius*, n.d.). India's economy is soaring, but its healthcare system remains an Achilles' heel.

.

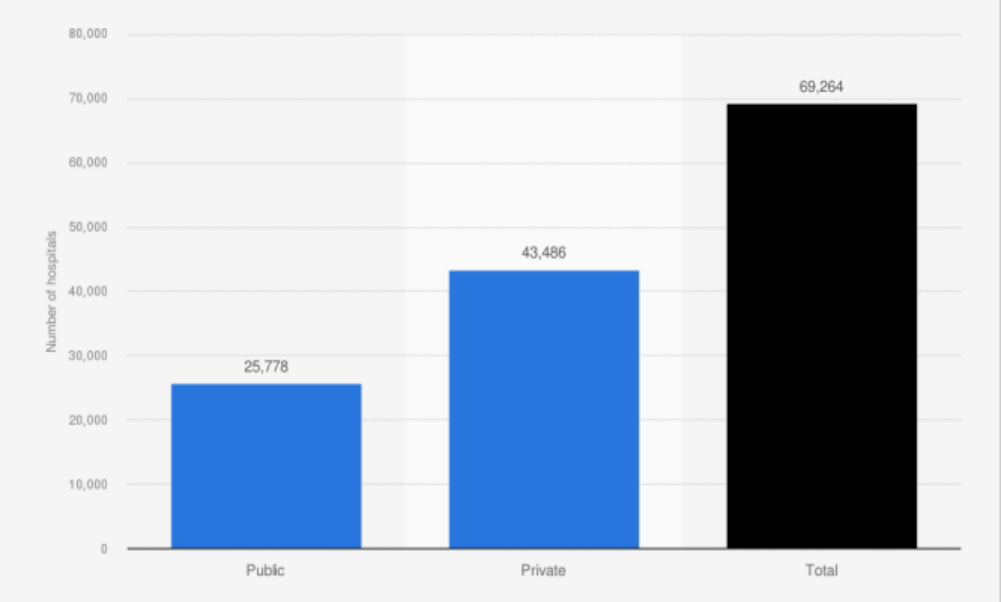

Figure 2.3 Estimated number of public and private hospitals across India in 2019

A physician, medical practitioner, medical doctor, or simply a doctor, is a professional who is concerned with promoting, maintaining, or restoring health through diagnosis, prognosis, and treatment of disease. Doctors are one important agent through which that scientific understanding is expressed. If we look the situation of India, then there are 241 doctors available for the 10,000(*India: Number of Doctors per 10,000 Population by State | Statista*, n.d.) population that are very less in contrast to population size. Though shortage of primary health providers has been hyped, India faces a severe shortage of specialists both for its rural and urban services and to strengthen its position in the medical world. Also, if we look state wise the distribution of doctors is also uneven across the country, with a low ratio in states like Chhattisgarh and Jharkhand.

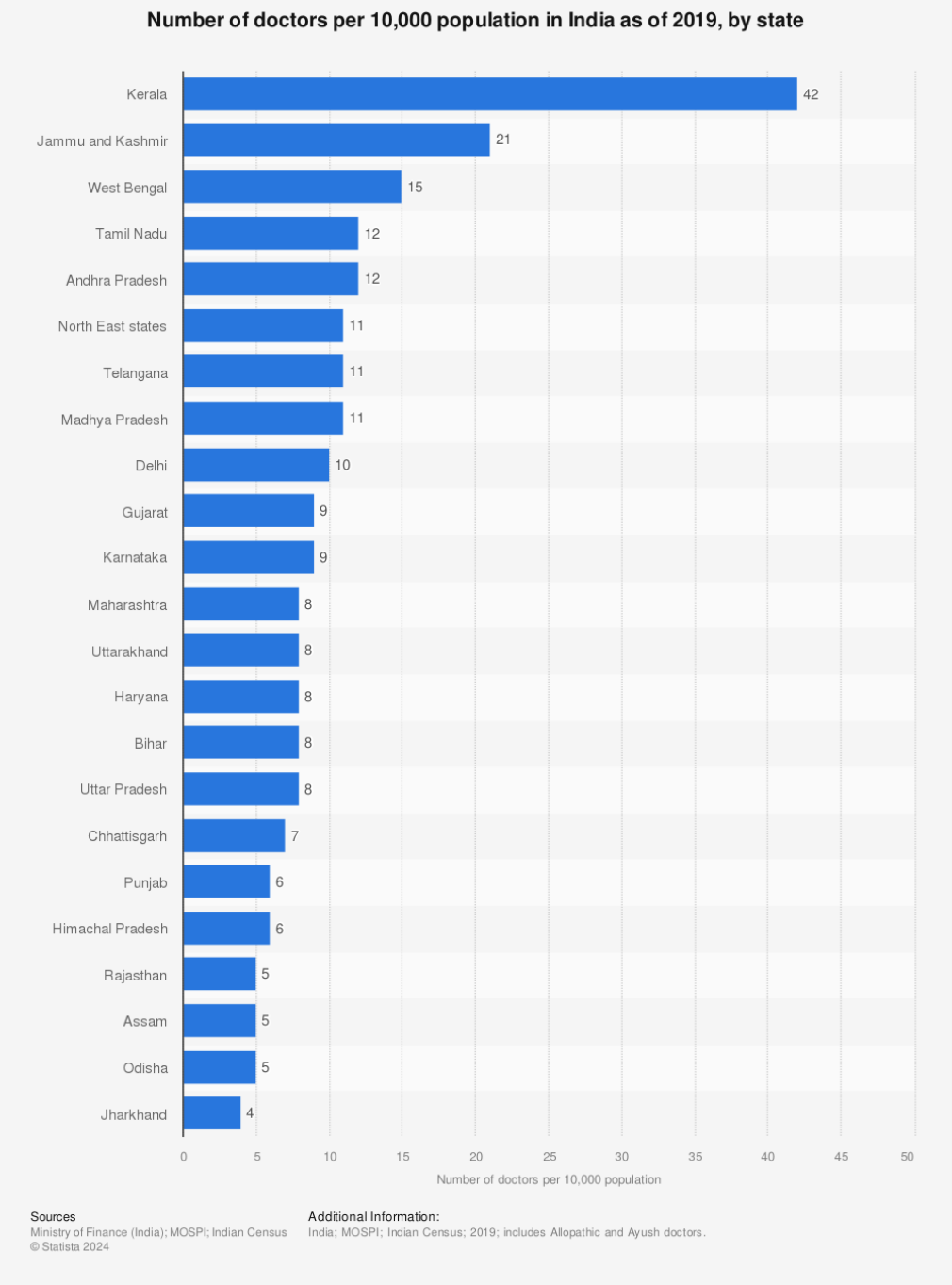

Figure 3.3 Number of doctors per 10,000 population in India as of 2019, by state.

To diagnose and treat patients, doctors currently rely on or use antiquated procedures and approaches that are ill-equipped to deal with novel diseases like the COVID-19 virus and a variety of new cancer subtypes, much alone offer answers. The conventional techniques and medical electronic instruments employed in diagnostic procedures are prone to inaccuracies whether measuring blood pressure, sugar levels, or capturing X-ray images.

When brain surgery is performed, clinicians encounter challenges in accurately identifying areas of heightened neural activity inside the brain(*Technology Is Changing How Doctors Diagnose, Treat Patients*, n.d.). They anticipate that the country would focus on the development of high-tech medical procedures like well-equipped intensive care units, cardiac bypass surgery, organ transplants, advanced imaging technologies (MRI, PET), prenatal diagnosis, newborn screening, in vitro fertilization (IVF), etc.

India is witnessing fast demographic changes which will soon results in a deluge of lifestyle disorders (cardiovascular and neurological disorders, diabetes, and cancer, *etc*.). By 2025, India may become the world's diabetic capital(*India--Diabetes Capital of the World: Now Heading towards Hypertension*, 2007).

In the healthcare sector, patient records were managed with a paper-based management system. These records help check the patients' day-to-day activities and observe how patients respond to the line of treatment given by the doctor. Many small pieces of information are in records that are very sensitive and essential for doctors. All this information mentioned in the medical record also needs to be protected and secured because all this patient-related data come under sensitive data which is covered under IT Rule(*Rule 3: Sensitive Personal Data or Information*, 2011) 2011. Further, these records act as a shield for the administration of the hospital in the future if any legal obligation by the side of the party of the patients. All the records are so confidential and for that hospital, administrators need to take special precautions like separate infrastructure for storing records and protecting them from unauthorized use. After all these practices there are many cases where documented form patient records got misplaced and misused. Results impacted directly on the patient's lives, and a new method is required which is more secure and easily accessed by doctors globally.

3.2.1. Need to embrace new technologies

The healthcare industry is crucial to the prosperity of the country and the general welfare of society. The level of development of a nation can be gauged by the quality of its healthcare system, hence it is critical that all problems in this area be solved quickly.

The major concern is diagnosing patients through medical instruments. Because of the diagnosing and medical errors, the number of Americans dying each year is around 98,000 more than those who die from, breast cancer, or AIDS(America et al., 2000). The American public is dissatisfied with chronic care; 72 percent of those surveyed believe it is difficult for people living with chronic conditions to obtain the necessary care from their healthcare providers(*Harris Interactive Inc. -- Company History*, n.d.). Health professionals are also concerned: 57 percent of U.S. physicians surveyed said their ability to provide quality care has been reduced in the last 5 years, and 41 percent stated that they are discouraged from reporting or not encouraged to report medical errors(Blendon et al., 2001); 76 percent of nurses surveyed indicated that unsafe working conditions interfere with their ability to deliver quality care(*American Nurses Association*, n.d.). A survey of over 800 physicians found that 35 percent of physicians reported errors in their own or a family member's care(Blendon et al., 2001).

While a British National Health System survey in 2009 reported that 15% of its patients were misdiagnosed, an American study published in the Journal of the American medical association in 2000. Also, there are 2000, death every year from unnecessary surgeries, 7000 deaths from medication errors in hospitals, 20,000 from other machines errors in hospitals, and 106,000 deaths every year from non-error, adverse effects of medications. If we look globally, in the US 225,000 deaths occur per year due to unintentional medical errors(*Medical Errors in Top 10 Killers: WHO | India News - Times of India*, n.d.). So, after all these incidents, the first question that comes to mind is who will be responsible for all the incidents? If we look around, there is no specific rule or regulation that concerns patient safety in hospitals. Over 100 million people require surgical treatment every year. Problems associated with surgical safety in developed countries account for half of the avoidable adverse events that result or disability. There is a need for regulation as well as new advanced technology that helps to reduce the mortality rate by securing and implementing devices that are error-free.

In the absence of new technology, or poorly designed systems, the resulting lack of integration is apparent across sectors, as well as within individual

healthcare organizations. Such systems can harm patients or fail to deliver what patients need. When patients are moved from one setting to another for example, from hospital to rehabilitation center to home fragmentation of care results in overlapping or conflicting treatment that is costly and confusing and, worst of all, detrimental to the patient. In a recent survey, 85 percent of physicians surveyed stated that one or more adverse outcomes result from uncoordinated care, and more than half suggested that a lack of coordination is usually the cause of patients receiving contradictory health information from providers(Anderson et al., 2002).

The method of keeping records that is followed in most hospitals globally is the manual method involving paper and books. Most clinical information is still stored in a collection of poorly organized and often illegible paper records.

The commonly used practice of utilizing paper-based systems for the storage of patient data, although traditionally prevalent, poses numerous difficulties within the modern healthcare environment. The manual retrieval of paper data is characterized by a high degree of inefficiency, which frequently leads to delays that can have a major influence on the provision of medical care. The physical area used by these tangible records becomes increasingly substantial as the number of patients increases, necessitating the implementation of extended storage systems. In addition, it should be noted that paper records are vulnerable to a range of potential damages, including water and fire damage, as well as general deterioration, which poses a significant danger of permanently losing essential patient information. Another issue of concern is legibility, as handwritten notes have the potential to be misinterpreted, leading to medical blunders. The use of paper-based systems restricts accessibility, as it allows only one individual to access a file at any given time, hence hindering the joint endeavors of medical teams. The security of these documents is a significant problem, as paper records lack the encryption measures seen in digital solutions, rendering personal patient information susceptible to unauthorized access, duplication, or theft. Furthermore, the ecological impact of persistent paper consumption, encompassing deforestation and garbage

generation, is substantial, giving rise to apprehensions regarding sustainability. In conclusion, although paper-based systems have been utilized by the medical community for many years, their inherent limitations emphasize the necessity for contemporary digital alternatives.

3.2.2. Patient Medical Records: Concerns and Problems

Medical records are helpful to patients because doctors encounter numerous people every day and can't possibly keep track of all the details of each individual case in their heads. The current patient could become ill again in the future, be admitted to the same hospital or to another hospital with a different ailment and be seen by the same doctor or by a different doctor(Adeleke et al., 2014). The medical record is the who, what, why, where, when, and how of the patient care during hospitalization(*Medical Record Management : Huffman, Edna K., 1896- : Free Download, Borrow, and Streaming : Internet Archive*, n.d.).

The patient's medical record serves as the source of information for a wide variety of reasons, such as the sole record of accomplishment, the only measurement of the work being done by the medical and nursing staff, and the only record of the patient's progress. The exponential growth of data and information, especially in the healthcare industry, is well-documented. With a growing population, a greater volume of patients, and the appearance of new diseases and symptoms, healthcare providers must collect and handle massive volumes of data and information(Desouza, 2005).

A patient's medical record is "a confidential record that is kept for each patient by a healthcare provider or organisations," as defined by Haux(Haux, 2006) (2006). Information such as the patient's name, residence, and date of birth are included, as well as a synopsis of the patient's health history and detailed accounts of each incident, including symptoms, diagnoses, treatments, and outcomes. All supporting paperwork and correspondence are supplied as well. Back in the seventeenth century, Adeleke(Taiwo Adeleke, 2015)explains, In 1752 A.D. Benjamin Franklin set up an incorporated Hospital and starts storing patient's records in Philadelphia in the United State of America. This event marked a significant milestone in the evolution of medical records. At the moment, the brand name for this establishment is Pennsylvania Hospital.

By compiling a case file in which patient's names, admission dates, discharge dates, etc. were noted, he pioneered the medical record.

On the other hand, hospitals typically keep several different kinds of medical records, as Durkin(Durkin, 2006) (2006) elucidated by naming the following categories of information:

i. Patient History and Examination report.
ii. Consultation report.
iii. Operative report.
iv. Radiology report.
v. Pathology report.
vi. Laboratory report.
vii. Emergency report.
viii. SOAP note report (Subjective, Objective, Assessment & Plan notes.
ix. Progress notes report.
x. Therapy report.
xi. Clinical notes.
xii. Autopsy report.
xiii. Biopsy report.
xiv. Psychiatric observations.
xv. X-ray report.
xvi. Scan report.
xvii. Referral letters.
xviii. Daily report.

The patient's medical history is one of the most vital instruments for sharing information about the treatment they have received. They also contribute greatly to our understanding of illness epidemiology, which has far-reaching implications for the health of a nation's healthcare infrastructure. The medical record is useful to hospitals since it documents the staff's level of expertise. The hospital's efficiency and effectiveness can be evaluated in terms of patient outcomes. As Berg(Berg, 2001)explains, If it is correctly created and maintained medical record by the hospital then it will be used by a practitioner's primary defense and an advocate in any official or legal process. This is of great benefit to the hospital from a medical-legal standpoint(Berg, 2001).

Medical or patient data are particularly sensitive, which has created a few problems with administrative oversight. The most frequent ones have to do with conveniences like easy access and a secure environment for your belongings. A lack of space is a common issue for hospitals that rely predominantly on paper-based medical record-keeping systems. Another difficulty users and administrators have is gaining access to medical records.

The issue might arise over who has access to and who should pay for a patient's medical records. This tension has been attempted to be lessened by the *US Fair Health Information Practice Act of 1997*(*Fair Health Information Practices Act of 1997* , n.d.), which mandates that healthcare providers grant patients access to their medical records and provides security to the healthcare record. For non-compliance of guidelines issued by the authority, the hospitals get punished with civil and criminal penalties (Trudel et al., 2017).

Securing patient health data poses the biggest challenge for medical professionals. In 1996, Nicholson(Levin & Nicholson, 2005) found many examples when this was the case, where patient records were not stored safely. In according to Nicholson's own examples, had that been true, it would have been simple for spies to get into case studies found in public databases or elsewhere a free-for-all: places where authorities have no say. Evidence, such as case notes, unsupervised in out-of-hospital settings, and in some cases kept overnight in clinic waiting areas because medical records in the office was now closed.

It is important for all practitioners (doctors, nurses, medical secretaries, ward record keepers, administrative assistants, and others) to be aware of the importance of safety and protection. Moreover, Nicholson(Levin & Nicholson, 2005) argued that computer terminals, particularly when unattended, should not be left accessible, along with fax machines and consistently under-secured and unregulated computer systems. The challenges encountered in health information management are closely associated with the improper handling of medical records. To what extent can the absence of appropriate record-keeping methods in the medical field, when employed as safety measures, lead to potential abuses and the heightened risks of privacy breaches and confidentiality concerns pertaining to clinical documentation?

The administrative or the authorities that keep patients' records face a challenge when it comes to the confidentiality of their medical files. According to Nicholson(Levin & Nicholson, 2005), there were numerous cases in which case notes were not stored in a safe place. The case notes in several of Nicholson's cases may have been easily accessed by unauthorized individuals thanks to the prevalence of such materials in public places like

libraries. For example, after hours, when the medical records department had closed, case notes would be left in the clinic locations where they had been created, even though no one was there to take care of them. The researcher emphasized the significance of security for all case note users (doctors, nurses, medical secretaries, ward clerks, medical records employees, and others). Nicholson also noted that fax machines and poorly protected and monitored computer networks pose a threat, as can unattended computer terminals, especially if they are left logged on.

A breach of patient privacy and confidentiality may occur if medical records are not managed effectively, and adequate safeguards are not in place. 'The confidentiality of medical records is jeopardized in many ways, among others who are worried about the inappropriate use of medical data. The most sensational cases of medical data theft and release have included individuals seeking either financial gain or revenge.

The United States was the first country to establish rules and regulations regarding the preservation or maintenance of patient data to standardize these issues of medical record storage and patient privacy. The Health Insurance Portability and Accountability Act 1996 (HIPPA) was the first piece of legislation that was introduced during the peak time when the existing laws were proving to be insufficient. It's fair to say that HIPAA, or the Health Insurance Portability and Accountability Act, is among the most consequential pieces of healthcare legislation ever passed in the United States. Health Insurance Portability and Accountability Act (HIPAA) was enacted by Congress and signed into law by President Bill paper-based 1996 to ensure that individuals in between employment may continue to maintain health insurance coverage. Later many other countries were inspired by the step taken by the US. After the US many countries came forward and looked upon the issues of keeping patient medical records secure and protecting the patient's privacy.

In India the issue of storing medical record is again a herculean task which have been addressed in the Medical Council of India Regulations and guidelines (*Code of Medical Ethics Regulations, 2002 | NMC*, n.d.) of 2002,

it has answered questions regarding the medical records of healthcare. The issues which are addressed by the regulations are mentioned below:

i. Maintain indoor records in a standard proforma for 3 years from the commencement of treatment (Section 1.3.1).
ii. Request for medical records by patient or authorized attendant should be acknowledged and documents issued within 72 hours (Section 1.3.2).
iii. Maintain a register of certificates with the full details of medical certificates issued with at least one identification mark of the patient and his signature (Section 1.3.3).
iv. Efforts should be made to computerize medical records for quick retrieval (Section 1.3.4).

The accountability in a case of misuse of a medical record is not specified in Medical Council of India regulations. In the event of a violation of patient medical records, compromising privacy and confidentiality, there is currently no legislation in place that effectively protects the rights of patient privacy. The existing loophole in the legislative framework of India necessitates attention and scrutiny.

The primary objective of the regulations set forth by the Medical Council of India is to ensure the proper maintenance of medical records and adherence to established standards. However, in the event of an unfortunate incident such as an incident with fire that results in the loss of medical records or failure to adequately safeguard them, it is important to determine the party liable and assign liability accordingly. The matter at hand pertains to the allocation of accountability between doctors, hospital administration, or both parties. The absence of legislation, policies, rules, and regulations in India pertaining to liability provisions was discovered by the researcher in relation to the question.

The confidentiality of the patient's information is of utmost importance, as it is imperative to uphold their right to privacy by refraining from releasing it to the public. Each individual patient possesses the entitlement to ensure and uphold the confidentiality of their medical records. The health care industry is confronted with a significant struggle in securely and privately preserving the growing volume of patient's medical records. The patient's record in

question possesses legal validity and admissibility in court as documented evidence due to their inherent resistance to tampering, which makes it challenging to alter them without leaving any discernible traces of modification.

There are many studies conducted regarding the documentary medical reports stated that paper-based medical reports are a hassle(Morris, 2020). The usage of paper-based records as a method for record-keeping is deemed to be ineffective and characterized by a slow pace, rather than being regarded as efficient, timesaving, and expedient. Medical personnel dedicate a significant amount of time to documenting patient data, owing to many factors. Professionals are required to physically transcribe all written content, a laborious task that poses the risk of data loss due to the absence of numerous copies. The utilization of paper charts in medical record keeping introduces the potential for errors or mistakes, which can undermine the overall reliability of the records. Healthcare practitioners are actively seeking an alternative to the current methods, and fortunately, Electronic Health Records (EHRs) have emerged as a viable solution that holds potential for global acceptance(*The Disadvantages of Paper Medical Records*, n.d.). The state authorities in the United States are currently exploring more effective methods for managing medical information and are considering the implementation of a new system known as electronic medical records.

3.3. Role of the Government in the Healthcare sector

The healthcare system in various nations is widely regarded as being in a state of disarray, necessitating the ruling government's obligation to assure the efficient provision of healthcare services. The primary role of these entities is to establish and uphold standardized levels of care on a nationwide scale, formulate comprehensive initiatives to cater to the requirements of the entire nation, and provide sufficient resources to facilitate the advancement, supervision, and provision of healthcare services. The primary responsibility of the government is to promote equitable access to healthcare services for all individuals, while also promoting effective coordination among various levels of the healthcare system. It is imperative to devise a system or strategy that facilitates prompt reaction and minimizes waiting periods. It is imperative for

governments to prioritize the provision of support and protection for disadvantaged populations within society.

To ensure that all nations have access to adequate healthcare facilities, a national plan is needed to track the supply and demand of healthcare professionals and to create policies to support these experts. The healthcare sector's success and future trajectory can be significantly influenced by the involvement of governments. Proper allocation of resources, adherence to legal frameworks, and the establishment of a consistent standard are vital.

Medical research should be supported by the government as well to reduce the shortage of medical professionals. This objective can be accomplished through the provision of backing for medical research and the subsequent translation of discoveries into policies and practical applications.

The right to health is somewhat discussed in International Law and fundamental Human Right in India's Constitution under umbrella Article 21(*Article 21: Protection of Life and Personal Liberty* , n.d.), this also encompasses the rights to life, liberty, and the pursuit of happiness.

A definition of health that encompasses *a person's mental, emotional, and social well-being rather than just the absence of disease or infirmity* may be found in the preamble of the World Health Organization's (WHO) Constitution, which was first written in 1946. Every person, regardless of their ethnicity, religion, political affiliation, or socioeconomic status, has the right to '*enjoy the best possible quality of health'* stated explicitly by WHO(*Human Rights*, n.d.).

Article 25(*Article 25: Right to Adequate Standard of Living*, 1948) of Universal Declaration of Human Rights 1948, stated the Right to Adequate Standard of Living. This article's stated goal is to protect everyone's right to a standard of living sufficient for their health and well-being in the face of unemployment, sickness, disability, widowhood, old age, or any other lack of livelihood. This includes the right to food, clothing, housing, medical care, and necessary social services.

In the International Covenant on Economic, Social, and Cultural Rights (ICESCR), the right to health was again recognized as a human right. According to Article 12 of the International Covenant of Economic, Social,

and Cultural Rights(*International Covenant on Economic, Social and Cultural Rights | OHCHR*, 1966), '*the right of everyone to the enjoyment of the best achievable quality of bodily and mental health'* is a relative definition of the right to adequate health.

Despite extensive research and analysis on the significance of healthcare at both national and international levels, there remains a lack of consensus among authorities regarding the fundamental minimum standards for health-related rights that should be universally upheld. Furthermore, it is imperative to establish a minimum requirement for a robust healthcare sector, which includes essential services such as adequate treatment and investment in research and development to ensure a better future.

3.3.1. Importance and need of healthcare expansion

Technology, of course, is the leading business sector. Almost half of all Venture funding goes to the technology sector, and a 135% increase in output is expected over the next few years. The Market predicted that cloud computing, artificial intelligence and machine learning, and big data would have the most significant effects on the industry. Technology has changed and will continue to change the trajectory of every business, which is a primary reason for that industry's predicted success. Here's one example: the health industry, which ranks second.

Even though many hospitals and primary care facilities are in crisis and experiencing declines in profitability (especially in rural areas), the future output of the health industry as a whole look strong, thanks to the subsectors of biotechnology, health data management, and personalized health solutions, which are based on the idea that your health data will drive your immediate and long-term treatment options. A gold mine awaits the day when health care is individualized in the same way that entertainment and hospitality are now(Hecht, 2018).

It has become clear that the healthcare industry's current operational structure is inadequate to meet the needs of the public and that there is a gap in the industry's performance. Further, it is not easy to safely secure the numerous patient files that doctors, and hospital administrators must save on paper-based form.

Moving on, there is malfunctioning in the output values of devices used by doctors and lab assistants, meaning that they must operate on the entire body, even if it's just a small part, to get the job done. To find a solution, the old, inefficient system must be abandoned in favor of a new approach that is more equipped to handle these problems and meet the needs of modern society.

The healthcare industry is not exempted from the trend of automation that has expanded to other sectors of our society. From patient registration, patient monitoring from anywhere, and the inducement of the Internet of Things, Blockchain, Artificial Intelligence, the robotics, it's become clear that advancements in the industry have been a game-changer in making many tasks easier, while also making registration processes quicker and more accurate(*Advancements in Healthcare Technology - Benefits for Today's Healthcare Students*, 2022).

3.4. Innovations in Healthcare Sector

Technology and science are the two important essential instruments for socio-economic development. The advancement of technology played a fundamental role in the growth and development of different areas in industries. It may be the agriculture sector, Automobiles, Healthcare, Energy Sector, etc., and they are rapidly adopting new technology including the Internet of Things, Artificial Intelligence, Blockchain, and Robotics. These technologies help industries to give them a new shape and take each nation's economy to the next level.

In the healthcare sector, technology plays a very important role and replaces the traditional method of working. It is integral to the assessment and helps people to connect with a doctor using smart devices. It also helps with access to vital information and can enhance communication.

By utilizing the technology in making a smart healthcare system, the quality of storing patient records, the treatment process(Shao et al., 2010), and the interaction of patient-doctors become easier. Healthcare Industry is still an emerging trend in the sense that all its benefits and capabilities have not been completely explored(Lederman, Ben-Assuli, et al., 2021) and many areas need to explore.

3.4.1. Integrating technology into healthcare sector/ Adoption of Electronic Medical Record

The first step toward technological advancement is replacing the paper-based patient report method with an Electronic Medical Record (EMR). As inadequacies of the paper record became increasingly more apparent in 1992(*Ornstein, S.M., Oates, R.B. and Fox, G.N. (1992) The Computer-Based Medical Record Current Status. Journal of Family Practice, 35, 556-565. - References - Scientific Research Publishing*, 1992), the Institute of Medicine advocated a shift from a paper-based to an electronic medical record. However, the widespread use of this method is delayed and after 2009, it was again accepted widely by different nations. Most countries in Europe and the USA are increasingly using an Electronic Medical Record (EMR) due to the belief that it can help improve healthcare quality.

Electronic Medical Record (EMR) systems are defined as 'an electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff within one health care organization'(*Electronic Medical Record Systems | Digital Healthcare Research*, n.d.).

The patient's medical history(Moores, 2012) is stored in an electronic medical record (EMR) or electronic health record (EHR) system. This includes the patient's admittance note, progress notes, treatment orders, surgery information, test results, and more examination findings and a synopsis of the patient's medical record, which may include a breakdown of expenditures. With the use of a hospital's knowledge base, which may be facilitated by the introduction of an electronic medical records system, healthcare delivery and documentation could be enhanced(Adler, 2004). Researchers in the fields of healthcare and information systems are becoming increasingly interested in exploring the massive dataset created by the constant use of electronic medical records. Scholars in the healthcare field can benefit greatly from EMR systems because of their ability to quickly retrieve a patient's medical history in response to a specific ailment(Lim et al., 2012). Additionally, hospital administrators rely heavily on the data recorded in the system to assess the facility's performance and inform their decision-making. Researchers in the

field of information systems view EMR as an information technology (IT) initiative for measuring and forecasting things like hazards, hospital performance, and service level(Liu, 2016). There are two ways in which an electronic medical record system aids in the efficient and effective running of a hospital(Hillestad et al., 2005).

One of the primary functions of electronic medical records is to improve communication between patients and different parts of a clinic(Tierney et al., 2013). Then, electronic medical records (EMR) appear to have revolutionized healthcare by reducing expenditures for both outpatients and hospitalized patients(Hillestad et al., 2005). Reid(Evans, 2016) recommends using electronic medical records (EMR) to cut costs in the healthcare sector, since the data collected by these systems can greatly cut down on redundancy, such as repeated examinations, and provide better care for patients with chronic conditions. Buntin et al.(Buntin et al., 2011) agree, noting that hospitals use of EMR systems has the potential to slow the rise in healthcare costs. The electronic medical record (EMR) is much more than just a handy piece of information technology that helps doctors update and retrieve patient records more quickly and easily(Thompson, 2013). When EMR is combined with social media and cloud computing, it provides a knowledge platform that may be used to better understand patients with specific diseases and enhance clinical practice(Lau et al., 2012).

When compared to the paper-based method, the EMR system is more convenient for doctors, more reliable, and less prone to error. From anywhere with the internet connectivity, doctors with the patient's unique I'd has reviewed the record. The electronic medical record is a pioneering effort that has already shown great promise in healthcare. After the implementation of EMR system, other IT giants began to enter the healthcare market with the introduction of innovative new technologies in the healthcare sector.

The healthcare market in India will grow rapidly between 2008 and 2022 (Figure 3.5). Over the past two years, there has been a significant market growth of 178 billion US dollars, with the lowest decline observed during the period of 2011-2012. Between the years 2008 and 2022, it is projected that the healthcare sector would experience a substantial increase in income

amounting to $327 billion. This notable figure serves as evidence of the considerable interest exhibited by prominent online companies in this area. The increase of the healthcare market can also be attributable to the development and implementation of innovative fusion healthcare technologies. The healthcare industry plays a crucial role in facilitating a country's economic development and ensuring overall progress.

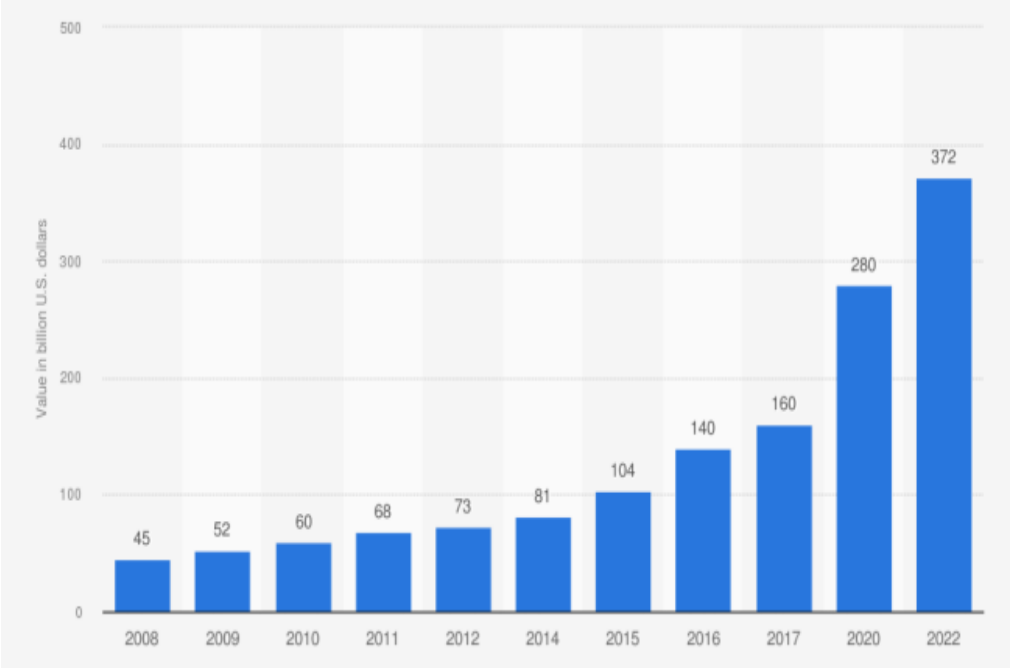

Figure 3.5 Size of the healthcare market in India from 2008 to 2020, with an estimate for 2022(in billion U.S. dollars(Minhas, 2023)*)*

The subsequent impetus for technological progress in healthcare has led to more attention being paid to the technologies of Internet of Things, Big Data Analytics, blockchain, Cloud Computing, and Artificial Intelligence. When we look on a global scale, it's clear that every country is making significant strides to improve its healthcare system. Countries with a stronger focus on

healthcare infrastructure development are among the top 10 in the world (table 3.1).

1	Country	Citations	Link Strength
2	China	491	32
3	India	269	21
4	Pakistan	93	21
5	Saudi Arabia	110	21
6	United Kingdom	169	17
7	United States	166	16
8	Sweden	17	13
9	Slovakia	0	12
10	Australia	94	9
11	South Korea	98	9

Table 3.1 List of top 10 countries

China has the top position in Table 3.1, as depicted in the aforementioned display. Within this framework, citations function as the fundamental criteria upon which a nation's comprehensive rating is established. Based on the available data, it can be observed that China's advancements in the healthcare sector have been highly influential, serving as a source of inspiration or a model for healthcare systems in 491 nations. This suggests that China's healthcare Research and Development (R&D) is of exceptional quality on a global scale. India is ranked second, which is a commendable achievement. India's global affiliations, as illustrated in the accompanying Figure 3.6, exhibit robustness.

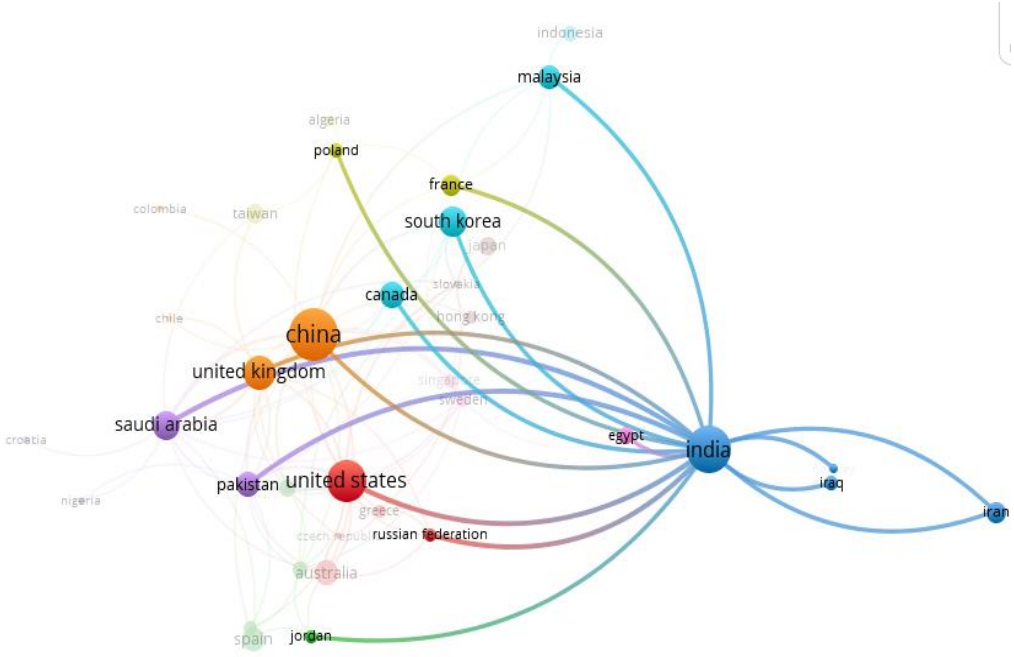

Figure 3.4 Cluster of India with the other nations

This cluster in Figure 3.6 emphasizes the success of the Indian healthcare sector by highlighting the nation's contributions to and support of the development of healthcare technologies abroad. India possesses the second-largest population globally; nonetheless, in contrast to other prominent nations, its healthcare system exhibits deficiencies. The Indian healthcare system is in dire need of creative technological advancements that might alleviate the burden on healthcare professionals. The healthcare sector is endeavoring to adapt to contemporary advancements by integrating state-of-the-art technologies into their routine practices. The Internet of Things (IoT)

1	Keyword	Occurrences	Link Strength
2	Internet of Things	1450	11449
3	Network Security	179	1784
4	Energy Utilization	133	1424
5	Energy Efficiency	132	1354
6	Deep Learning	136	1301
7	5g mobile communication systems	131	1295
8	Edge Computing	135	1249
9	Machine Learning	134	1177
10	Blockchain	126	946
11	Digital Storage	95	900

is an advanced technology that has been extensively adopted in the medical domain.

Table 3.2 List of most occurrence keywords

The occurrences and link strength discussed in Table 3.2 above lead to the development of two major ideas. The findings of the literature review indicate that the term "Internet of Things" was referenced a total of 1,450 times across the articles included in the study. Furthermore, the link strength associated with this term was measured to be 11,449. Undoubtedly, the Internet of Things (IoT) has emerged as a widely embraced instrument for driving innovation in the healthcare sector. A technology connection score of 11,449 for the Internet of Things indicates a high level of integration with several technologies, including network security, machine learning, and blockchain.

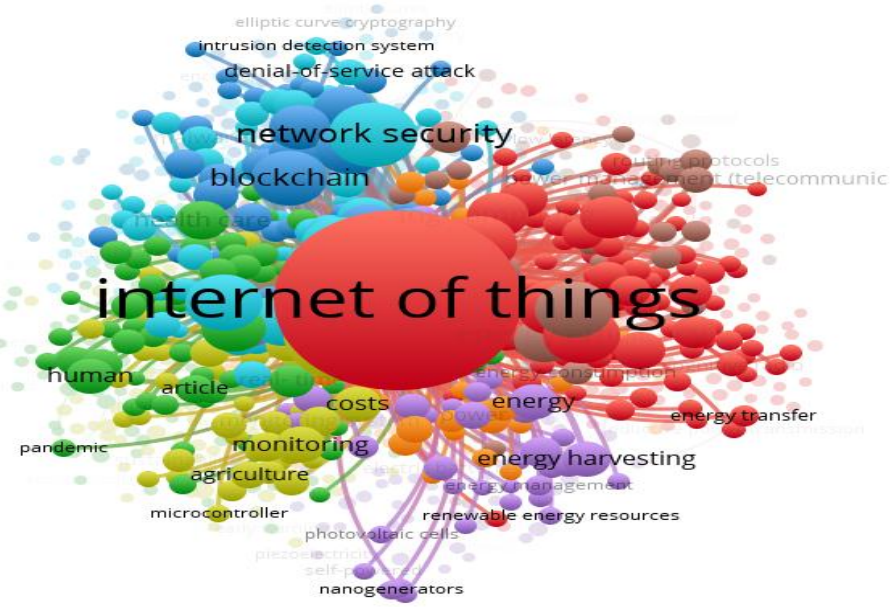

Figure 3.5 Cluster of IoT in relation with other keywords

Using IoT to advance medical technology as demonstrated in the cluster Figure 3.7 up top. A wide range of software, applications, smart systems, tools, and cloud storage solutions are interconnected through the Internet of Things (IoT) technology. The Internet of Things (IoT) refers to a network comprising physical objects, commonly known as things, which are embedded with electronics, including sensors, software, and other

technological components. The primary objective of these objects is to facilitate communication and data exchange with other networks and devices, such as smartphones and computers, via the internet. The Internet of Things (IoT) plays a significant role in advancing human health. The possibility of establishing a remote connection between doctors and patients for the purpose of information sharing is viable.

3.4.2. Internet of Things (IoT) Applications

The healthcare sector has expanded rapidly in recent years, becoming a significant source of both economic and job growth(Ali et al., 2018). Miniaturized gadgets like smartwatches can now be used for health monitoring and disease diagnosis because of technical progress over the years. In addition, technological advancements have shifted the focus of healthcare away from hospitals and onto individual patients(G. Yang et al., 2014). Several clinical studies (such as measuring blood pressure, blood glucose level, pO2, and so on) can be done at home without the assistance of a healthcare expert. Furthermore, with the help of modern telecommunication systems, clinical data can be transmitted to healthcare institutes from faraway locations. Access to healthcare facilities has been enhanced using such communication services in tandem with rapidly developing technology (such as machine learning, big data analysis, the Internet of Things (IoT), wireless sensing, mobile computing, and the cloud).

To monitor and exchange data with other physical equipment, the IoT devices (sensors, actuators, etc.) have been integrated with them using various communication protocols such as Bluetooth, Zigbee, IEEE 802.11 (Wi-Fi), and so on. Embedded or wearable sensors are used to capture data from the human body for use in healthcare applications(Li et al., 2014). This data can include the patient's temperature, blood pressure, Electrocardiogram (ECG), Electroencephalogram (EEG), and other physiological readings. The time, date, temperature, and humidity of a given location can also be recorded. These records allow for more informed conclusions to be drawn about a patient's health.

3.4.2.1. Services of IoT are

i. **Ambient Assisted Living (AAL):** To aid the elderly, a subset of AI has been developed called Ambient Assisted Living (AAL), which makes use of the Internet of Things (IoT). An elderly person's emergency detector developed by Sandeepa in a recent study helps keep tabs on their chronic conditions and other possible health emergencies. More importantly, the system notified the attendants if there was a problem(Sandeepa et al., 2020). Assistive robots have made it possible for Internet of Things-based healthcare systems to monitor interior air quality. Systems like this monitor the air quality around a patient's home(G. Marques et al., 2019) and notify medical staff if it drops below a certain threshold.

ii. **Wearable Devices:** Wearable devices help healthcare professionals and patients to deal with various health issues at a reduced cost. These devices are noninvasive and can be developed by integrating various sensors with wearable accessories used by humans such as watch, wristband(L. Zhao et al., 2018), necklace, shirt, shoes, handbag, caps, and so on(Pradeep & Sharma, 2020). The sensor attached is used to collect the environmental and patient's health information. This information is then uploaded to the server/databases. Some wearable devices are also connected with mobile phones through health applications. Jie in his research have developed an IoT-enabled health monitoring device where several sensors (including heartbeat, body temperature, and blood pressure sensors) have been embedded to provide remote health monitoring. Bio signals such as electrocardiograph (ECG) and electromyography (EMG) signals were also analyzed with the help of IoT enabled wearable systems to extract patient's vital information(Pantelopoulos & Bourbakis, 2010). The interconnectivity of these wearable devices with a mobile application enhances the computational power of the device. The application can be further used for easy processing and visualization of the collected information.

iii. **Adverse Drug Reaction:** An Adverse Drug Reaction (ADR) can be characterized as a side effect of taking a medication. The reaction may occur either after a single dose or a long-term administration. This can also be possible due to the adverse reaction when two different medicines are ingested

at the same time. ADR does not depend on the type of medicine, or the disease and it varies from person to person. In an IoT-based ADR system, a unique identifier/barcode is used to identify each medicine at the patient's terminal(Jara et al., 2010). The information about the drug's compatibility with the patient's body can be checked using a pharmaceutical intelligent information system. The information system stores the allergy profile of each patient using e-health records. After analyzing the allergy profile and other vital health information, a decision is made whether the medication is suitable for a patient or not. In a similar study(Nakhla et al., 2019), an IoT-based Prescription Adverse Drug Event (PRESCADE) system has been proposed, which can improve patient safety by reducing the ADE.

iv. **Child Health Information**: Child Health Information (CHI) is a concept that deals with creating awareness for a child's well-being. The main purpose of CHI is to educate and empower children and their parents on the child's overall health including their nutritional values, emotional and mental state, and behavior. Nigar and Chowdhury have developed an IoT-based framework where a child's mental and physical state can be monitored(Nigar & Chowdhury, 2018). The system collects five different body parameters: height, temperature, SpO2, weight, and heart rate.

v. **ECG Monitoring**: Electrocardiogram (ECG) represents the electrical activity of the heart due to the depolarization and repolarization of atria and ventricles. An ECG provides information about the basic rhythms of the heart muscles and acts as an indicator for various cardiac abnormalities. These abnormalities include arrhythmia, prolonged QT interval, myocardial ischemia, etc. The use of IoT technology has found potential application in the early detection of heart abnormalities through ECG monitoring. The study reported in(Rahman et al., 2022) has proposed an IoT-based ECG monitoring system that is composed of a wireless data acquisition system and a receiving processor. It employed a search automation method that was used to detect cardiac abnormality in real time. It is worthy to note that in(Djelouat et al., 2020) system was designed to provide real-time monitoring to elderly patients by continuously checking their ECG and accelerometer data.

vi. **Glucose Level Monitoring:** Diabetes is the condition in which the blood glucose level in the body remains high for a prolonged period. It is one of the most common diseases in humans. The most widely used diagnostic method for the detection of diabetes is “fingerpicking” followed by the measurement of blood glucose level. The recent development in IoT technologies has been used in designing various wearable gadgets for blood glucose monitoring that is noninvasive, comfortable, convenient, and safe(Nguyen Gia et al., 2019).

vii. **Temperature Monitoring**: Human body temperature is an indicator of the maintenance of homeostasis and is an important part of many diagnostic processes. Additionally, a change in body temperature can be a warning sign in some illnesses such as trauma, sepsis, and so on. Keeping track of the change in temperature over time helps the doctors to make inferences about the patient’s health condition in many diseases. The conventional way of measuring temperature is using a temperature thermometer that is either attached to the mouth, ear, or rectum. But the low comfortability of the patient and the high chances of contracting an infection are always an issue with these methods. However, the recent development in IoT-based technologies has proposed various solutions to this problem. In(Ota et al., 2017), a 3D printed wearable device was proposed that could be worn on the ear, which tracks the core body temperature from the tympanic membrane using an infrared sensor. The device was integrated with a wireless sensor module and data processing unit.

viii. **Blood Pressure Monitoring:** One of the compulsory procedures in any diagnostic process is the measurement of Blood-Pressure (BP). The most accustomed method of measurement of blood pressure requires at least one person to do the recording. However, the integration of IoT and other sensing technology has transformed the way BP was previously monitored. For example, in(Xin & Wu, 2017), a wearable cuffless gadget has been proposed that can measure both systolic and diastolic pressure. The recorded information can be stored in the cloud.

ix. **Asthma Monitoring**: Asthma is a chronic illness that can affect the airways and may cause difficulty in breathing. In asthma, the airways shrink due to the swelling of the air passage. This follows many health issues such as wheezing,

coughing, chest pain, and shortness of breath. There is no suitable time for an asthma attack to come, and an inhaler or nebulizer is the only lifesaver at that moment. Hence, there is a potential need for real-time monitoring of this condition. Numerous IoT-based systems for asthma monitoring have been proposed in recent years(Guler et al., 2018). In one the study(Shah et al., 2019), a smart healthcare solution for asthma patients was proposed that was used to record respiratory rate using a smart sensor. The health information was stored in a cloud server that gives access to caregivers for diagnostic and monitoring purposes. Raji in its work, proposed a respiratory monitoring and alarm system where an LM35 temperature sensor was used to measure the respiratory rate(Raji et al., 2016). This was achieved by monitoring the temperature of the inhaled and exhaled air. The respiration data were sent to the health center and were displayed on a web server. The proposed system also triggered an alarm and automatically sent a message to the patient once a threshold value was reached.

x. **Medication Management:** Medication adherence is a common issue in the healthcare industry. Non-adherence to the medication schedule may increase the adverse health complications in patients. Medication non-adherence is mostly found in elderly people as they develop clinical conditions like cognitive decline, dementia, and so on as the age progresses. Hence, it is difficult for them to strictly follow the prescriptions of doctors. Numerous research in the past has focused on tracking the patient's compliance with medication through the application of IoT(Aldeer et al., 2018). In, a smart medical box was developed that can remind people of their medication. The box has three trays where each tray contains the medicine for three different times (morning, afternoon, and evening)(Bharadwaj et al., 2017). The system also measures some of the vital health parameters (blood glucose level, blood oxygen level, temperature, ECG, and so on). All the recorded data is then sent to the cloud server. A mobile app was used to establish communication between the two end-users. The recorded information can be accessed by doctors and patients using the mobile app. One of the more specific examples of medication management is "Saathi"(Pradhan & Chawla, 2020). This pill

monitoring system was specifically designed for woman going through in vitro fertilization (IVF) treatment.

xi. **Other Notable Applications:** The application of the Healthcare Internet of Things (HIoT) is disparate and not limited to the aforesaid functions. With the rapid growth of technology, the number of HIoT applications is increasing significantly. Some of the research areas where the integration of IoT devices was not explicitly demonstrated previously are now using this technology efficiently. This may include cancer treatment, remote surgery, abnormal cellular growth, hemoglobin detection, etc. In(Heshmat & Shehata, n.d.), a new IoT-based framework for cancer treatment was proposed that integrated various stages of cancer treatment including chemotherapy and radiotherapy. A mobile app was used for online consultation from doctors. The lab-test results of patients were stored in the cloud server and could be accessed by the healthcare provider to decide the time and dosage of medication. Another potential application is the detection of lung cancer using various state-of-the-art machine learning algorithms with an IoT-based system(*Fog Computing Employed Computer Aided Cancer Classification System Using Deep Neural Network in Internet of Things Based Healthcare System. - Abstract - Europe PMC*, n.d.).

There are numerous applications in the domain of IoT such as smart healthcare systems(Nikooghadam, Amintoosi, & Kumari, 2021), smart homes, smart transportation, smart agriculture, and smart cities in this digital world(Malarvizhi Kumar et al., 2021). In the smart healthcare system, one of the most used applications is smart wearable.

Smartwatches can display the wearer's heart rate, pulse, steps taken, and much more. These devices are built with wireless sensors, which send data to a cloud database. Then the rough data is arranged using different algorithms and that data is sent to the individual who wants to know. Low-cost disposable patches based on IoT, generally worn for a couple of days, are known as fabric and flexible devices. Biostamp, iRhythm, BP monitor, UV sense, and electro pads are examples of flexible disposable patches(Paul et al., 2021).

Data of patients collected remotely using necessary IoT devices for various diseases such as cancer, heart, and diabetic diseases. The various kinds of IoT

devices that incorporate suitable sensors used for collecting the symptoms of cancer, diabetes, and heart diseases including the glucose level, heartbeat rate, ECG values, etc. The important features have been collected and stored as separate records for all the patients with patient identification numbers. The collected data will be forwarded into the cloud database(Malarvizhi Kumar et al., 2021).

3.4.3. Artificial Intelligence (AI) in Healthcare Sector

The delivery of healthcare is being revolutionized using artificial intelligence (AI) and machine learning technologies. There are massive amounts of information stored by health institutions, including patient records and photographs, population statistics, claims data, and information from clinical trials. Technologies based on artificial intelligence (AI) are ideally suited to examine this data and find patterns and insights that people would be unable to detect on their own. By leveraging AI's deep learning capabilities, healthcare providers may enhance the quality of care they deliver to patients and the satisfaction of their customers.

AI is gradually changing medical practice. There are several AI applications in medicine that can be used in a variety of medical fields, such as clinical, diagnostic, rehabilitative, surgical, and predictive practices. Another critical area of medicine where AI is making an impact is clinical decision-making and disease diagnosis. AI technologies can ingest, analyse, and report large volumes of data across different modalities to detect disease and guide clinical decisions(Hamid, 2016).

However, as Meskò(Meskó et al., 2017) in his research shows, the technology will potentially reduce care costs and repetitive operations by focusing the medical profession on critical thinking and clinical creativity.

3.4.3.1. Application of AI in Healthcare Sector

i. **Health service management**: One of the notable aspects of AI techniques is potential support for comprehensive health services management. These applications can support doctors, nurses, and administrators in their work. For instance, an AI system can provide health professionals with constant,

possibly real-time medical information updates from various sources, including journals, textbooks, and clinical practices(Tran et al., 2019). AI applications allow, for example, hospitals and all health services to work more efficiently for the following reasons:

- Clinicians can access data immediately when they need it.
- Nurses can ensure better patient safety while administering medication.
- Patients can stay informed and engaged in their care by communicating with their medical teams during hospital stays.

ii. **Predictive Medicine:** Another relevant topic is AI applications for disease prediction and diagnosis treatment, outcome prediction and prognosis evaluation(Agrawal et al., 2018). Because AI can identify meaningful relationships in raw data, it can support diagnostic, treatment, and prediction outcomes in many medical situations(Agrawal et al., 2018). It allows medical professionals to embrace the proactive management of disease onset. Additionally, predictions are possible for identifying risk factors and drivers for each patient to help target healthcare interventions for better outcomes(Hamid, 2016). AI techniques can also help design and develop new drugs, monitor patients, and personalise patient treatment plans(Mehta et al., 2019).

iii. **Clinical decision making:** AI applications could support doctors and medical researchers in the clinical decision-making process. According to Jiang(Jiang et al., 2017a), AI can help physicians make better clinical decisions or even replace human judgement in healthcare-specific functional areas. AI technologies can support medical professionals in their activities and simplify their jobs(Panch et al., 2018).

iv. **Patient data and diagnostics:** AI techniques can help medical researchers deal with the vast amount of data from patients (i.e., medical big data). AI systems can manage data generated from clinical activities, such as screening, diagnosis, and treatment assignment. In this way, health personnel can learn similar subjects and associations between subject features and outcomes of interest(Jiang et al., 2017b). These technologies can analyse raw data and provide helpful insights that can be used in patient treatments. They can help doctors in the diagnostic process; for example, to realise a high-speed body

scan, it will be simpler to have an overall patient condition image. Then, AI technology can recreate a 3D mapping solution of a patient's body. For diagnostics, AI techniques can make a difference in rehabilitation therapy and surgery. Numerous robots have been designed to support and manage such tasks. Rehabilitation robots physically support and guide, for example, a patient's limb during motor therapy(Novak & Riener, 2015). For surgery, AI has a vast opportunity to transform surgical robotics through devices that can perform semi-automated surgical tasks with increasing efficiency.

In AI, human being coding device, setting instruction according to their requirement and then AI machines can think like humans and act like supercomputers. It can detect illness faster and with better accuracy. Through the history of a patient's electronic healthcare records AI can assist the patients about their possible illness that may cause serious health problems in future and suggest its possible care, treatment, and medications(Knickerbocker et al., 2018)(Kalita & Emilia, 2018).

In 2021, the artificial intelligence (AI) in healthcare market was worth around 11 billion U.S. dollars worldwide as shown in Figure 3.8(Stewart, 2023). It was forecast that the global healthcare AI market would be worth almost 188 billion U.S. dollars by 2030, increasing at a compound annual growth rate of 37 percent from 2022 to 2030.

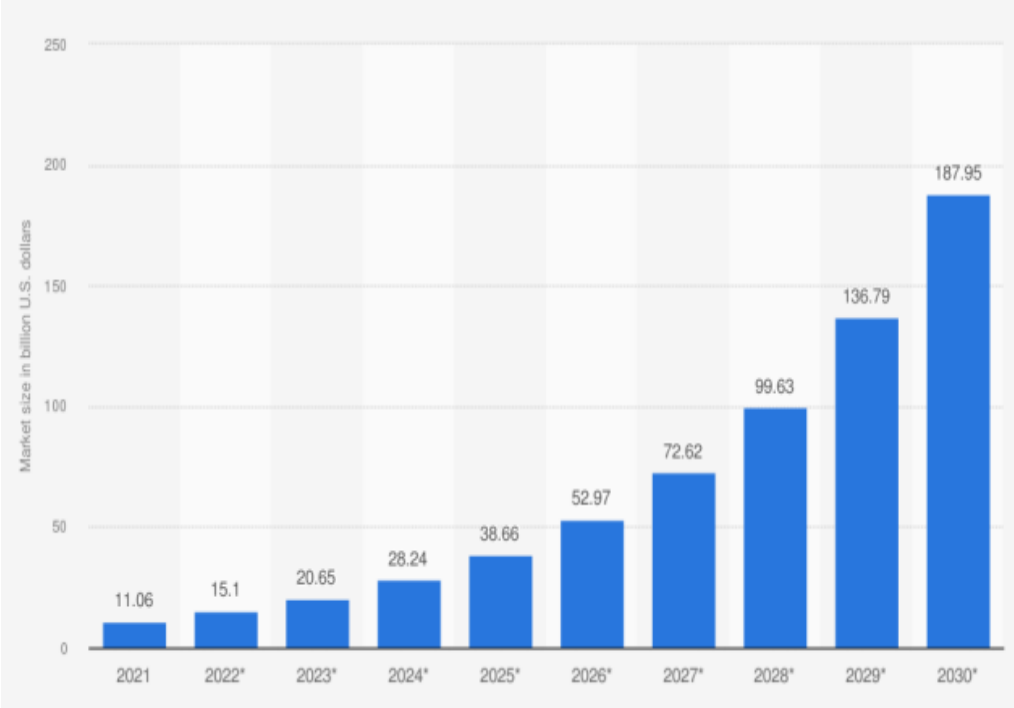

Figure 3.6 Artificial intelligence (AI) in healthcare market size worldwide from 2021 to 2030(in billion U.S. dollars)

Doctors analyse and diagnose the abnormalities from the registered patients tissue samples collected in different forms like images like scan reports, X-ray reports, and smears with the help of Artificial Intelligence (AI) models. As AI models can be able to diagnose affected tissues by analyzing a huge data set of the same kind within a fraction of time that can speed up the further treatment procedure. Once the patients get registered in the hospital system, then they can collect their reports, submit bills, and can visit concerned doctors remotely via mobile devices. Doctors can be able to provide medical support to the registered patients remotely(Mohanta, 2019).

Also, AI helps in the diagnosis and detection of COIVD-19. Robotics-based treatment can be conducted on patients using AI to reduce the risk for doctors using virtual reality(Haleem & Javaid, 2019).AI can detect any problem that the patient is suffering immediately, by using various sensors. AI technology has been proven as the best technology in the peak time of COVID and provides the best solution in detection of COVID.

3.5. Technology proposed as a Pandemic guard

The global outbreak of the novel coronavirus 2019 was declared by the WHO(*TECHNICAL FOCUS: Laboratory Detection*, 2020). There are no number of steps taken by the government to control the spread of the disease spread and finding treatment for it has failed. At that time, demand for global monitoring of patients and observing overall conditions.

During that IoT technology was proven as the best move to deal with the pandemic situation of COVID-19 and cope with the challenges during all the phases. In the first step, it will help to collect the data of COVID patients with that spread of the coronavirus can be controlled by early diagnosis(Ahmad et al., 2020). Then, to record the body temperature, various IoT-based smart thermometers are available. These IoT devices are available in different forms, such as radiometric, patch, and touch(Randazzo et al., 2021). IoT-based drones are also capable of monitoring COVID-19 infected patients and infected locations. It also reduces human interaction with each other and helps in reaching to the hard area locations in very less time(*How AI and Machine Learning Are Helping to Tackle COVID-19 | World Economic Forum*, 2022).

Healthcare Services	IoT Based Approaches	Conventional Approaches
Diagnosis and treatment	• Provide real time-based monitoring based on IoT applications and tools. • Reduces unwanted hospital visits and stays	• Patient monitoring process is very slow. • Patients are required to visit the hospital
Healthcare delivery	• IoT enabled drones are used for the supply of lightweights like vaccines and drug	• Patients are required to travel to buy the drugs

Disinfecting public spaces	• Provide real-time public space monitoring using IoT enabled drones	• Public space patient monitoring is very slow
COVID Linked Symptoms	• Emerging IoT based wearables help in detecting COVID symptoms	• To check or know about the symptoms patient needs to visit the hospital

Table 3.3 Examples of IoT and Conventional Application Usage during COVID-19 Management(Ferrag et al., 2021)

3.6. New challenges come during technological progress

The use of technology in the healthcare industry is a burgeoning trend that aims to improve the health and wellbeing of billions of people by providing streamlined medical facilities and upgrading the services offered by doctors, nurses, pharmaceutical companies, and other relevant government and non-government organizations.

But despite all these advantages for the healthcare industry, concerns about the privacy and security of patient information are expanding, often without the knowledge of either the patient or the medical staff. This is because the security and privacy of the Internet of Things devices and technologies are frequently disregarded and compromised by the manufacturer of the devices. Since the healthcare industry has advanced in technology innovation, there has been a dramatic increase in security breach cases. The main unresolved issue in the healthcare industry is the security and privacy of patient data kept in the cloud as well as data received during device connectivity. More so than ever before, according to recent figures, the healthcare industry tops all other industries in terms of recent cyberattacks, as depicted in Figure 3.9.

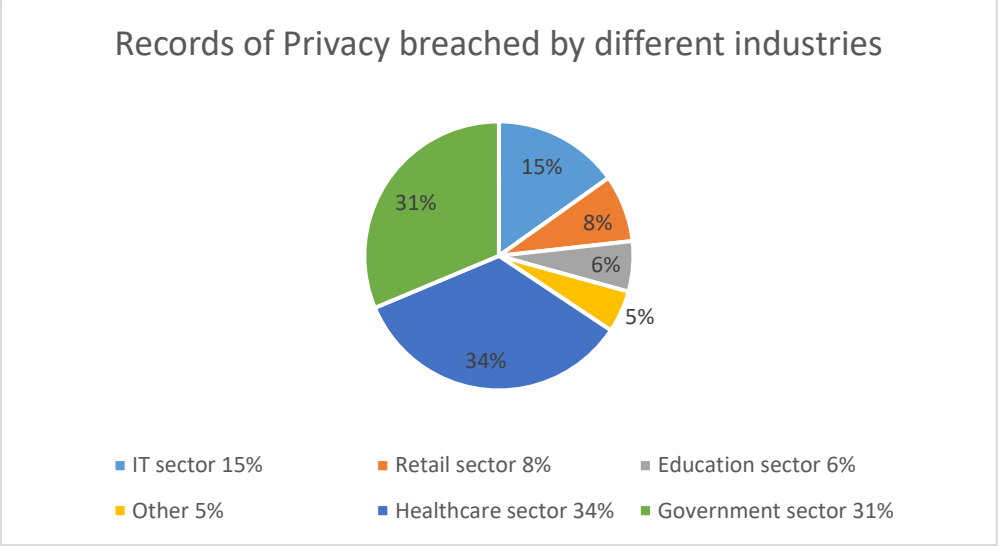

Figure 3.7 Statistics of the number of records breached by the industry(Asplund & Nadjm-Tehrani, 2016)-(Sun et al., 2018)-(Elhoseny, Thilakarathne, et al., 2021)

Doctors may readily reach patients through the new devices they are using and recommend the best course of action, but the biggest concern is that an attacker will intrude, access all the sensitive patient data, manipulate it, and thus easily threaten the lives of the patients. The attacker can misuse patient information by abusing or blackmailing them.

Most smart devices used by patients and clinicians contain sensors that can sense things like heart rates and blood pressure. It is incredibly simple for assailants to attack and kill the victim. Additionally, there are cyberattacks that harm the healthcare system because of outcomes like the alteration of sensitive data or information, data transmission delays, patient data monitoring, and the blocking of healthcare applications or smart healthcare devices or sensor control, patient profile control, or patient payment information theft.

All these situations show that there are insufficient regulations governing the modern healthcare system and that medical professionals, patients, and caregivers may all be at risk for vulnerabilities due to a lack of information and awareness. Many factors motivate attackers to continue abusing the technology employed in the healthcare sector, often putting patients' lives in jeopardy.

In the next part, the author examines the legal framework by which India is addressing the several problems that have arisen due to the healthcare sector's rapid development.

3.7. Conclusion:

This chapter delves into the analysis of the global healthcare system landscape. The healthcare sector operates on a worldwide scale, exhibiting an intricate and interdependent network that extends beyond national boundaries. This network involves a wide array of participants and encompasses various activities. Fundamentally, healthcare is propelled by a dedication to deliver medical care, foster overall health, and tackle global health issues. This study elucidates the operational mechanisms of both traditional and healthcare systems, as well as their respective approaches to patient diagnosis. After analyzing the previous research, it has become evident that the techniques and medical devices employed in the healthcare sector exhibit numerous flaws. There are numerous obstacles associated with the process of diagnosing patients and obtaining output data from electronic medical machines. These challenges include ensuring the security of patient medical information stored in paper based and accurately translating the obtained numbers into a chart or record. Consequently, patients frequently must traverse a disorganized network of healthcare professionals and services, leading to the fragmentation of care. The absence of integration can result in inefficiencies, redundant testing, and inadequate coordination of comprehensive care. Furthermore, the topic of healthcare accessibility continues to be of utmost importance in numerous regions across the globe, characterized by notable discrepancies in healthcare provisions between urban and rural locales, as well as among diverse socioeconomic strata. The issue of affordability is a prominent worry considering the ongoing escalation of healthcare expenses, which imposes a substantial economic strain on both individuals and households. The prevalence of a fee-for-service framework in numerous conventional healthcare systems might create a tendency to prioritize quantity over quality, which may result in excessive utilization of medical services and a

disproportionate emphasis on disease treatment rather than preventive measures.

To address these issues, it is imperative to devise and implement novel methodologies and procedures. The researcher subsequently examines the impact of technology adoption on conventional healthcare practices, elucidating how it has facilitated physicians in providing patient care more efficiently. This paper examines and provides insights into the necessity of establishing a legal framework for smart devices within the healthcare industry. The review included a combination of bibliometric analysis and content analysis. The study revealed that technology plays a crucial role in the healthcare sector by showcasing its effectiveness and offering novel avenues for development. Healthcare firms are progressively embracing emerging technologies such as Artificial Intelligence (AI), Blockchain, and the Internet of Things (IoT), which are prevalent in numerous software and hardware solutions within the industry. The proliferation of modern technology has led to the widespread adoption of various home medical equipment, such as infrared thermometers and heart rate monitors, in individual's everyday routines. These devices have been employed for the purpose of quantifying significant physiological indicators such as heart rate and body temperature. In the context of smart healthcare, individuals can transfer their physical health data obtained from smart medical devices to a doctor, a self-service medical system. This facilitates the acquisition of expert healthcare advice. The rapid progression of technology has outpaced the development of corresponding regulations, leading to a dearth of rules and legislation to effectively handle the emerging problems and challenges. The utilization of intelligent devices in the healthcare sector is experiencing a notable rise, prompting certain nations to actively pursue the establishment of suitable standards and regulations. The implementation of new technologies necessitates the establishment of a comprehensive regulatory framework or legislation to effectively address the various concerns that may develop.

The new healthcare sector has undeniably revolutionized the identification and management of patients, resulting in a multitude of advantages but simultaneously presenting a plethora of legal concerns and obstacles. A

significant subject that has garnered attention is the matter of data privacy and security. The proliferation of electronic storage and transmission of sensitive patient information has resulted in an elevated susceptibility to data breaches, so exposing healthcare organizations to significant legal ramifications and compromising the confidentiality of patients.

Furthermore, producers of smart devices are required to strictly comply with stringent requirements that stipulate the necessity of accessing the privacy area for all devices. The legal system needs to come up with new laws and policies that balance the new technologies like Internet of Things (IoT), Artificial Intelligence i.e., in the healthcare industry. Safeguarding patient-sensitive data holds significant importance within the healthcare sector owing to a multitude of crucial factors. The primary concern is the safeguarding of patient privacy and confidentiality. Medical records frequently encompass extremely sensitive data pertaining to an individual's health status, medical background, and therapeutic interventions. The act of gaining unauthorized access to this data has the potential to infringe upon a patient's fundamental right to privacy, so diminishing the level of trust placed in healthcare practitioners and potentially dissuading individuals from obtaining essential medical treatment. Additionally, attention should be given to investigating the implementation procedures of this framework by the diverse range of players involved. The subsequent chapter delves into the legal framework of India concerning the management of data protection concerns pertaining to electronic medical records within the healthcare industry.

CHAPTER 4

AN ANALYSIS OF EXISTING INDIA'S LAWS, RULES AND REGULATIONS PERTAINING TO ELECTRONIC MEDICAL RECORD AND UPGRADED MEDICAL DEVICES

4.1. Introduction

In a significant development, India has already surpassed China as the world's most populous country. Currently, India's population is 1.428 billion, slightly higher than China's 1.425 billion people, according to the UN's world population dashboard(*India Overtaking China as the World's Most Populous Country* , 2023). India to witness GDP growth of 6.0 percent to 6.8 percent in 2023-24, depending on the trajectory of economic and political developments globally. The optimistic growth forecasts stem from several positives like the rebound of private consumption a boost to production activity, higher Capital Expenditure (Capex), the healthcare sector, near-universal vaccination coverage enabling people to spend on contact-based services(*Information Bureau*, n.d.). The Indian healthcare market has been expanding at a compound annual growth rate (CAGR) of 22 percent because of the factors like population demographics, a growing middle class, rising incomes, better health awareness, and the number of new diseases.

The Indian healthcare market, which was valued at US$86 billion in 2016 is now projected to reach US$367 billion by 2023 and US$638 billion by 2025 as per *INC*. The healthcare sector in India is among major contributors to the Indian economy, in terms of both revenue and employment. The sector has grown rapidly in the last five years on account of digitization, innovation, and newer hybrid business models with the integration of traditionalists and technology enterprises.

India's healthcare sector comprises hospital infrastructure, medical devices and equipment, health insurance, clinical trials, telemedicine, and medical

tourism. These market segments are expected to diversify as an ageing population with a growing middle class increasingly favors preventative healthcare. The healthcare sector in India offers huge investment opportunities for both global and domestic investors. At present, there are 582 investment opportunities worth US$32.16 billion in the medical infrastructure sector(Bhardwaj, 2022).

The healthcare sectors are currently being significantly impacted by digitization, technology enablement, and automation. The healthcare delivery paradigm is undergoing a transformative shift and is on the verge of a significant advancement. The transformation of the healthcare industry and the advancements made in research and development within the pharmaceutical sector have significantly influenced the forefront of technological innovation. The healthcare system is expanding beyond the confines of conventional health departments as patient data is being seamlessly transferred between hospitals with a single click of the button.

By connecting patients and doctors online, the healthcare industry's integration with technology offers a solution for the future to people all over the world. In contemporary times, patients have the convenience of seeking medical advice through various mobile applications, thereby obviating the need for direct interaction with healthcare professionals.

The addition of technology in the healthcare sector not only enhances the quality of patient treatment, but also improves the whole patient care experience. Additionally, it is crucial to monitor advancements originating from peripheral entities such as technology corporations, as they have the potential to contribute to the field of diagnosis and early detection, thereby supporting the healthcare ecosystem. Significant efforts have been made over the past few decades to integrate information and communication technology (ICT) into medical operations(*Healthcare in India – 2022 and Beyond*, 2022). The widespread introduction of Information and Communications Technology (ICT) appears to be pervasive across several sectors. The field of information and communication technology (ICT) has significantly revolutionized the management of healthcare data(*Healthcare in India – 2022 and Beyond*, 2022). The proliferation of electronic devices such as laptops,

tablets, and mobile phones, along with the ubiquitous availability of high-speed internet, has facilitated the shift from traditional paper-based patient records to electronic records. Electronic Medical Records (EMRs) refer to contemporaneous digital renditions of patient records.

This chapter provides an overview of the legislative framework governing the regulation of data, specifically focusing on data protection legislation regarding electronic medical records (EMR), patient data and the medical device system. Furthermore, this paper will discuss the various concerns and obstacles associated with the implementation of Electronic Medical Records (EMRs). Subsequently, the implementation of enhanced technology in the healthcare industry. Finally, after the progress made in the healthcare industry, several concerns and obstacles have emerged.

4.2. Electronic Medical Records

Electronic Medical Records were first introduced in the 1960s, and their implementation starts in the 20th century. However, it is in the year 2009 when the "Health Information Technology for Economic and Clinical Health Act (HITECH)" was passed by the US and around $30 billion was allocated for the adoption of Electronic Health Records and its implementation on a large scale(Wadhwa, 2020). After this step, the EMR system will be adopted by many healthcare industries.

The subject of EMR comes up. In more precise words, an Electronic Medical Record (EMR) can be defined as a thorough documentation of an individual's complete health status. EMRs play a crucial role in monitoring patients clinical advancements, promoting enhanced healthcare decision-making, and delivering evidence-based care. Allocating time for the consequences of the information may have a generic quality, while in a different scenario, it may pertain to personal correspondence. If the information is of a public nature, the hospital may communicate information between departments without requiring prior approval from the patient. However, if the information is private, it is necessary to obtain the patient's consent beforehand.

A simple Electronic Medical Record System is shown in the Figure 4.1(*Electronic Health Records: Manual for Developing Countries*, 2006).

This includes details from some departments within the Institution. Depending on the scope of the EMR system patient details from other departments can also be included.

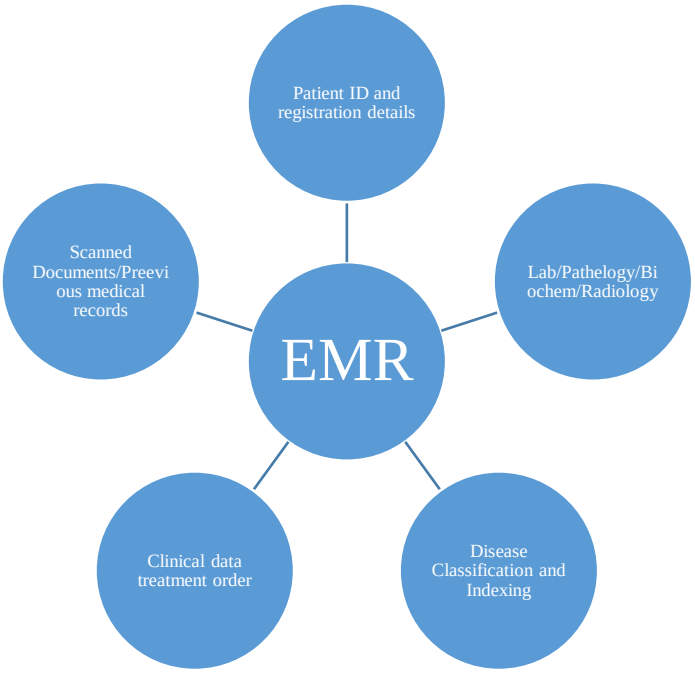

Figure 4.1 Simple Electronic Medical Record(*Electronic Health Records: Manual for Developing Countries*, 2006)

The use of an EMR helps to reduce medical errors by utilizing computerized prescription entry, predicting drug interactions, and displaying a warning for the health-care provider, assisting clinicians in reconciling patient medications, and most important, maintaining a detailed and legible medical record. Even though it takes longer to write the electronic clinical note than it would to write the same note by hand, in theory, visits guided by an electronic medical record should be shorter and more efficient. Another benefit of the EMR is that it allows clinicians to see patients in any order they like, with the most up-to-date information always being accessible. When using paper charts, this was a common source of frustration. In addition to providing quick access to patient records, EMRs also make it simple for physicians to enter prescriptions, lab orders, and other service requests into a centralized database, as well as keep track of related clinical notes. When compared to the storage requirements of the days of paper records, this is a significant

space saver. The patient's ability to access their own medical records quickly and conveniently from the comfort of their own home is another major benefit of this system. Electronic medical records also feature scheduling systems, which can help hospitals and clinics serve patients faster. The EMR technology also provides the doctor with instantaneous access to the diagnoses and opinions of other doctors. The EMR works well for everyone includes doctors, nurses, and patients(Alpert, 2016).

After implementing EMR, managing medications through an EMR improves patient outcomes over time. In fact, EMRs reduce adverse drug events by 52%(*HIT Safety: Progress Made and Challenges Ahead*, 2014). Some are designed to integrate with bar code scanning technology; if a nurse scans the wrong medication, an alert pops up alerting him or her to a problem. Critical lab values must be reported to the healthcare provider in a timely manner. The EMR flags each critical value for clinical staff, making notifications simpler for nurses. The EMR also helps clinicians determine when to repeat a lab test(*How Can Electronic Lab Results Help Me Improve Patient Care?*, n.d.). Another way an EMR improves treatment and clinical outcomes is by reducing the number of duplicate tests and improving overall efficiency(Hoover, 2017). The EMR also stores radiology results, which can be accessed from within the application if clinicians need to view the actual X-ray or the report from the radiologist(*Meaningful Use and the Shift to the Merit-Based Incentive Payment System*, n.d.). All reports are accessible to all clinicians involved in the patient's healthcare and can be viewed at any time. The patient medical report data is sensitive and private patient data. As the production of patient sensitive data increases with that the challenge of security and confidentiality sensitive data is difficult. Keeping patient records secure is one of the key challenges in the implementation of EMRs. There are concerns related to the misuse of the database and threat to cyber-security.

To ensure the privacy and confidentiality of the patient's record, access to data should be given only to authorized users. The chances of patient's identity theft are on rise because hackers may access and use someone else's identifiable information illegally to get medical services for the ailment. There was an instance reported that electronic medical records (EMR) of 35,000

patients held by a Maharashtra-based pathology lab were leaked, pointing to the lack of availability of adequate safeguards for protecting such sensitive information(Brown, 2023). The leaked medical records contain HIV reports. In cases of HIV patients, it gave details of CD4 count and viral load in the blood. CD4 count measures the level of immunity of an HIV-positive patient while the viral load gives a count of the virus in the blood. The website (www.hsppl.com) had over 40,000 files, of which an estimated 30,000 to 35,000 were related to patient's records. The leaked files had details such as patient's names, ages, gender, blood test report, lipid profile, and other medical parameters.

In 2022, there was a huge breach of patient records from the servers of AIIMS, affecting around 3 to 4 crore individuals. The inability of staff or doctors to obtain patient information such as medical history, prescriptions, and lab tests has a direct influence on the patient's life(*AIIMS Cyber Attack: EHospital Data Restored, Details of 3 Crore Patients Still at Risk amid Rs 200 Cr Ransom Reports*, 2022).In 2024, about 12,347,297 patient's private data was compromised by malicious attackers. The data includes patient's laboratory information as well as their financial details. The primary concern in this occurrence is the potential manipulation or alteration of sensitive patient data, which is a significant case of a data breach. In the dark web marketplace, healthcare records can be priced as high as 1,000 USD per record, while credit card data typically fetches a price of 5 USD. Health and medical data are attractive targets for hackers and cybercriminals due to their high value and the financial incentives they offer(*Millions of Highly Sensitive Patient Records Exposed in Medical Diagnostic Company Data Breach*, 2024).

4.2.1. Incorporation of cutting-edge technologies in healthcare care

The subsequent impetus for technological progress in healthcare has led to more attention being paid to the technologies of Internet of Things (IoT), Big Data Analytics, Blockchain, Cloud Computing, and Artificial Intelligence (AI). When seen on a global scale, it's clear that every country is making significant strides to improve its healthcare system and trying to keep up with the times by incorporating cutting-edge technologies into their daily

operations. Internet of Things is a cutting-edge technology that has found widespread use in the medical field (IoT). To monitor and exchange data with other physical equipment, the IoT devices (sensors, actuators, etc.) have been integrated with them using various communication protocols such as Bluetooth, Zigbee, IEEE 802.11 (Wi-Fi), and so on. Embedded or wearable sensors are used to capture data from the human body for use in healthcare applications(Li et al., 2014). This data can include the patient's temperature, blood pressure, electrocardiogram (ECG), electroencephalogram (EEG), and other physiological readings. The time, date, temperature, and humidity of a given location can also be recorded. The doctors diagnosed the patients using advanced medical devices and based on patient medical reports suggested further treatment.

Assistive robots have made it possible for Internet of Things-based healthcare systems to monitor interior air quality. Many IoT devices helps in monitoring the air quality around a home(G. Marques et al., 2019) and notify medical staff if it drops below a certain threshold. Bio signals such as electrocardiograph (ECG) and electromyography (EMG) signals were also analyzed with the help of IoT enabled wearable systems to extract patient's vital information(Pantelopoulos & Bourbakis, 2010). The use of IoT technology has found potential application in the early detection of heart abnormalities through ECG monitoring. The recent development in IoT technologies has been used in designing various wearable gadgets for blood glucose monitoring that is noninvasive, comfortable, convenient, and safe(Nguyen Gia et al., 2019).

Artificial Intelligence (AI) has also proven as revolutionary step in implanted in healthcare sector. Technologies based on artificial intelligence are ideally suited to examine this data and find patterns and insights that people would be unable to detect on their own. By leveraging AI's deep learning capabilities, healthcare providers may enhance the quality of care they deliver to patients and the satisfaction of their customers. AI technologies can ingest, analyse, and report large volumes of data across different modalities in diagnosing the diseases and helps in taking clinical decisions(Hamid, 2016). In AI, human being coding device, setting instruction according to their

requirement and then AI machines can think like humans and act like supercomputers. It can detect illness faster and with better accuracy. In pandemic, robotics-based treatment can be conducted on patients using AI to reduce the risk for doctors through the of virtual reality(Haleem & Javaid, 2019). AI can detect any problem that the patient is suffering immediately, by using various sensors and has been proven as best technology in the peak time of COVID-19 by giving solution for detection of COVID.

Despite all these advantages for the healthcare industry, there is a growing threat over the privacy and security of patient information, often without the knowledge of either the patient or the medical staff. Because of a lack of awareness, the security and privacy of the Internet of Things devices and technologies are frequently disregarded and compromised by important parties. Since the healthcare industry has benefited from technology innovation, there has been a dramatic increase in security breach cases.

The above-mentioned argument can be substantiated by taking because in 2023, the largest data breach incident in the United States was Anthem Inc. attack. This data breach caused the theft of private information of at least 78.8 percent of the individuals. The next big data breach case occurred at Optum360, LLC in 2019.

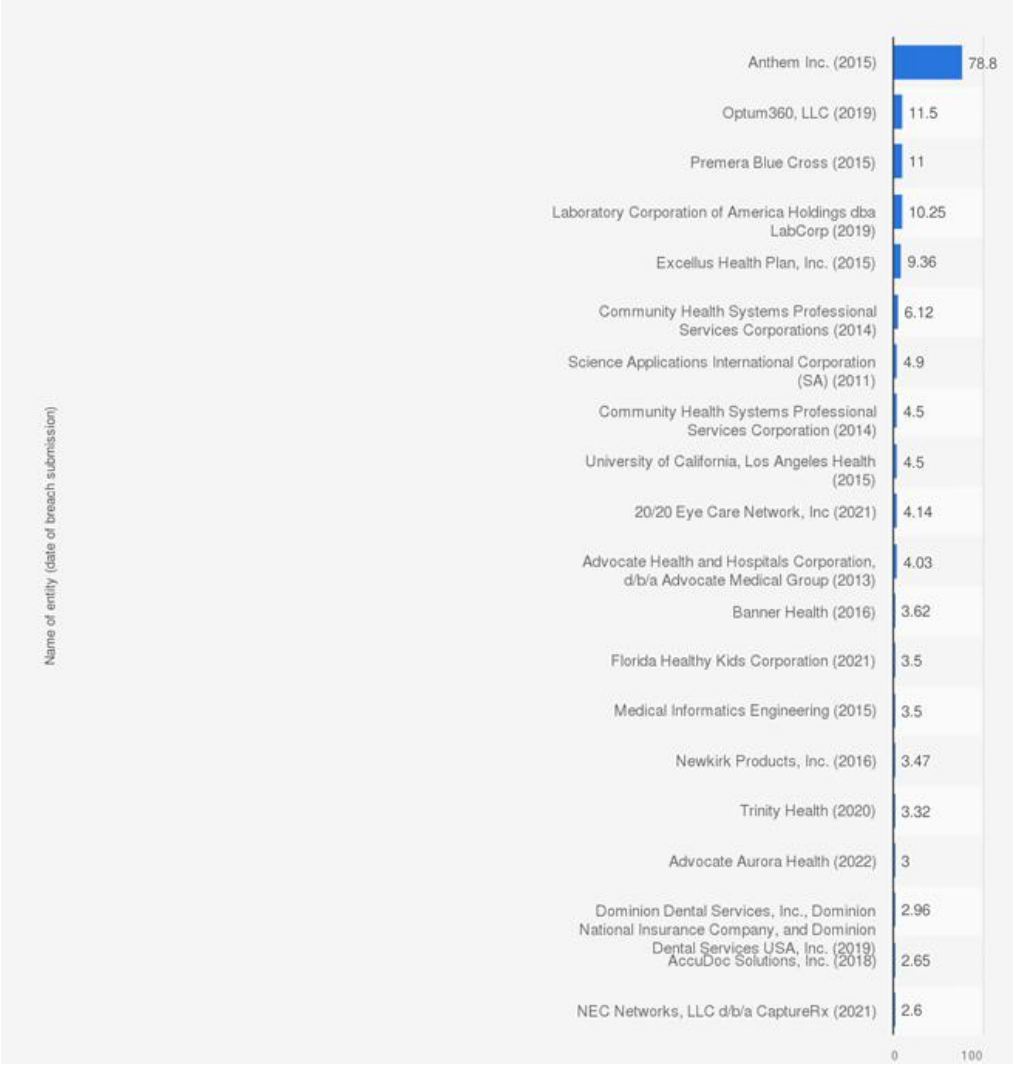

Figure 4.2 Largest healthcare data breaches to date in the United States as of May 2023, by number of affected individuals(in millions)(Petrosyan, 2023)

After taking the abovementioned happenings (where data was hacked or breached) into consideration, let's explore the ways in which the data could have been misused. The data could have been mistreated in the following ways:

i. **Misinterpretation of medical records**: In the smart healthcare system, doctors and patients are interconnected with smart wearables devices like patches, wrist band etc. These smart devices run with internet connectivity. All sorts of patient-doctor communication, line of treatment and recommendations take place through these smart devices. Since the smart devices run through internet connectivity, any third person can intrude and hear, manipulate, misinterpret, disclose the secret information shared during conversation through wireless channels. The attacker can easily get access to

all the sensitive patient data and manipulate it which can be life-threatening and fatal(Thilakarathne, 2020)-(W. Zhao et al., 2012).

ii. **Misusing and Blackmailing**: The attacker can easily get over the stored patient medical data and after that they can misuse the patient data in any way they want. They can sell their data on the black market, abusing(Dimitrov, 2016) patients and blackmail the patient by threatening to disclose his/her sensitive data to the public.

iii. **Threatening for life**: In healthcare, all the smart devices used by patients and clinicians contain sensors that can sense things like heart rates, blood pressure and so on. It is incredibly simple for the attacker to get access and handle these medical devices sensors(Mamdouh et al., 2021) and after that they can control the devices of the patients and cause the death of the patient.

iv. **Delay in the transmission of patient data**: Nowadays, all the patient data is transferred over the internet servers. The communication of the patient-doctor depends upon the data. Attacker, by interrupting the flow of communication of data delays in sending the patient info to the doctor's result in the starting of late medical treatment and directly affect the patient's health.

v. **Financial Theft**: All the patient's information is stored in clouds. That information consists of patient medical records, lab records, and financial details as well. Attackers use the financial details of the patient and get access to them. That leads to financial breaches or cyber theft.

vi. **Breach of Network Server**: The IoT device used by the patient relates to the Internet 24*7, and this device passes all the relevant patient information to the doctor that is on the other side. According to that sensitive information, the doctor prescribed the line of treatment. Now what attackers do is, attack the network layers and stop the entire communication channel due to the patient not getting treatment in a timely. That impacts somewhere to the patient's health or maybe the patient loses their life.

4.3. The Current Status of Indian Legislation

India has implemented many laws, rules, and policies to govern the management of patient privacy and the protection of data in the healthcare sector (Fig. 4.3). The legislative framework pertaining to Electronic Medical Record, Medical Device Regulation and the Patients Data Protection in India

includes several key acts and rules. These include the *Drugs and Cosmetics Act of 1940, the Drugs and Cosmetics Rules established in 1945, the Drugs Control Act of 1950, the amended Drugs and Cosmetics Act of 1964, the Indian Medicine and Central Council Act of 1970, the Medical Termination of Pregnancy Act of 1971, the Homeopathy Central Council Act of 1973, the MTP Rule of 1975, the Mental Health Act of 1987, the Transplantation of Human Organ Act of 1994, the Transplantation of Human and Tissues Act of 1994, the Drugs and Cosmetics (Amendment) Act of 2008, the Indian Medicine Central Council (Amendment) Act of 2010, the Clinical Establishments (Registration and Regulation) Act of 2010, the PDPB Bill of 2019, the Medical Device Rules of 2017, the Drugs, Medical Devices and Cosmetics Bill of 2022, the Digital Personal Data Protection Bill of 2022, the Digital Personal Data Protection Act of 2023,* and *the National Medical Device Policy of 2023*. The researcher conducts an analysis of each law to determine the state of legislation pertaining to patient data in the healthcare sector.

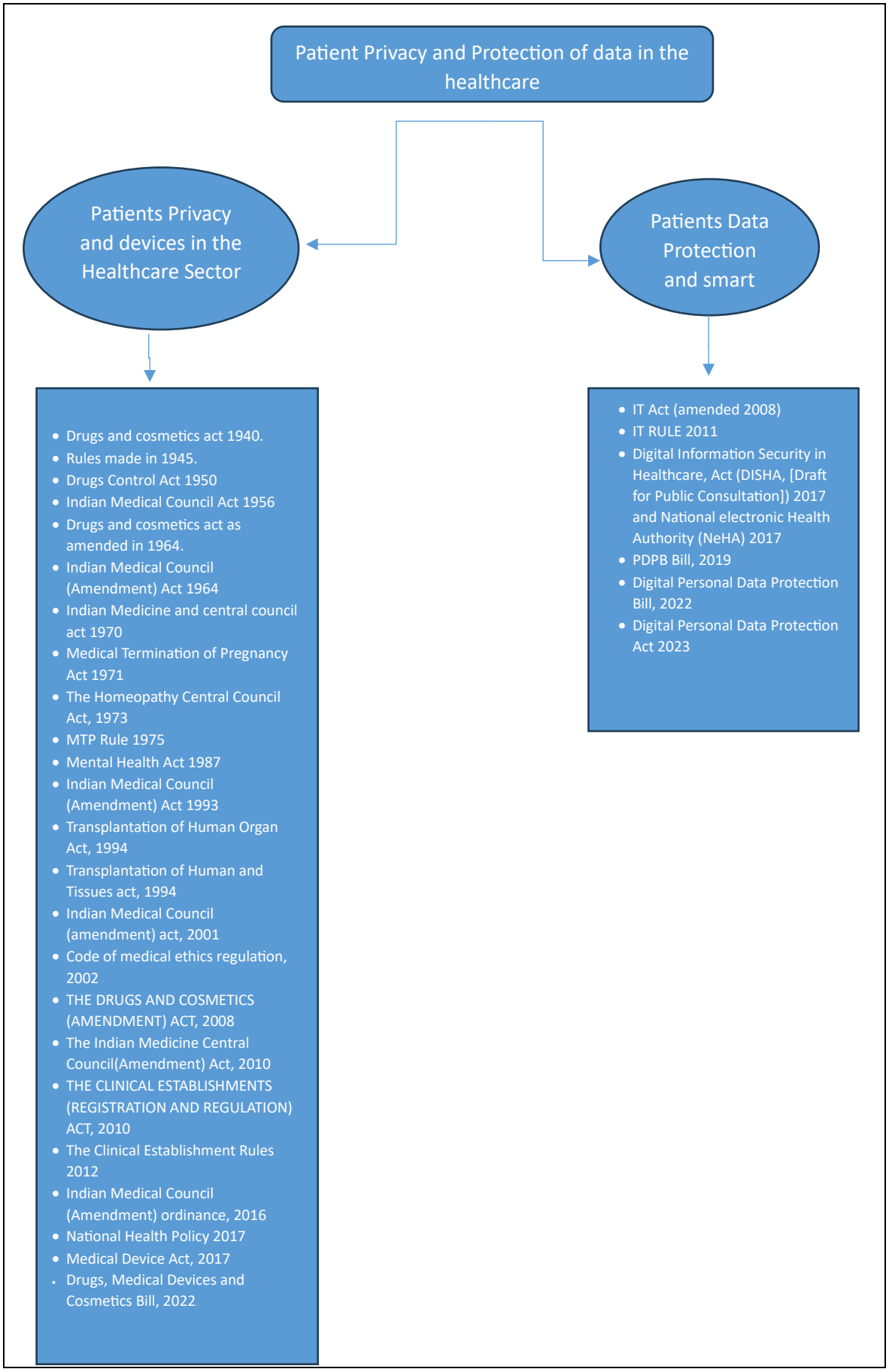
Patient Privacy and Protection of data in the healthcare
Patients Privacy and devices in the Healthcare Sector
Patients Data Protection and smart
Drugs and cosmetics act 1940.
Rules made in 1945.
Drugs Control Act 1950
Indian Medical Council Act 1956
Drugs and cosmetics act as amended in 1964.
Indian Medical Council (Amendment) Act 1964
Indian Medicine and central council act 1970
Medical Termination of Pregnancy Act 1971
The Homeopathy Central Council Act, 1973
MTP Rule 1975
Mental Health Act 1987
Indian Medical Council (Amendment) Act 1993
Transplantation of Human Organ Act, 1994
Transplantation of Human and Tissues act, 1994
Indian Medical Council (amendment) act, 2001
Code of medical ethics regulation, 2002
THE DRUGS AND COSMETICS (AMENDMENT) ACT, 2008
The Indian Medicine Central Council(Amendment) Act, 2010
THE CLINICAL ESTABLISHMENTS (REGISTRATION AND REGULATION) ACT, 2010
The Clinical Establishment Rules 2012
Indian Medical Council (Amendment) ordinance, 2016
National Health Policy 2017
Medical Device Act, 2017
Drugs, Medical Devices and Cosmetics Bill, 2022.
IT Act (amended 2008)
IT RULE 2011
Digital Information Security in Healthcare, Act (DISHA, [Draft for Public Consultation]) 2017 and National electronic Health Authority (NeHA) 2017
PDPB Bill, 2019
Digital Personal Data Protection Bill, 2022
Digital Personal Data Protection Act 2023

Figure 4.3 Classification of Privacy and Patient's Data

4.3.1. Rules, Regulation, and the laws specifically to Patient Privacy Rights and medical devices regulation in the Healthcare sector

A. Drugs and cosmetics Act 1940

The Drugs and Cosmetics Act of 1940 is a legislative enactment by the Indian Parliament that governs the importation, production, and dissemination of pharmaceuticals within the nation. The primary objective of this legislation is to guarantee the safety, efficacy, and compliance with state quality regulations of pharmaceuticals and cosmetics available in the Indian market.

The production and commercialization of pharmaceuticals is a regulated endeavor governed by the Drugs and Cosmetics Act of 1940 and the Drugs and Cosmetics Rule of 1945. Licensees are obligated to adhere to the provisions outlined in the act, as well as the norms and conditions specified by the licensing authority. These requirements pertain to the manufacturing and sale of pharmaceutical products. The Drug and Cosmetic Act of 1940 contains comprehensive provisions aimed at regulating the manufacturing of counterfeit and substandard drugs within the nation.

The Drug and Cosmetic Act of 1940 is the inaugural legislation that addresses the preservation of standards for cosmetics and drugs. It establishes a board of technical experts to offer guidance to both the central and state governments on matters of a technical nature. This Act specifically outlines guidelines pertaining to the distribution, manufacture, import, and sale of cosmetics and drugs. Additionally, it encompasses the regulation of Ayurveda, Siddha, and Unani drugs, as well as provisions related to these practices. Notably, this Act solely concentrates on upholding the quality of cosmetics and drugs, without incorporating any regulations concerning medical devices or instruments utilized for patient diagnosis.

The Drug and Cosmetic Act of 1940 includes a clause that serves to safeguard consumers, particularly by preventing the distribution of counterfeit and contaminated pharmaceuticals that are sold to government entities or utilized in state-run medical facilities. However, it is important to note that this legislation does not effectively safeguard the rights of patients in instances of

medical malpractice, namely pertaining to the malfunction or failure of medical equipment employed in the provision of healthcare services.

In Section 3(b) of the Drug and Cosmetic Act of 1940, the term "***drug***" is defined. Additionally, Section 3(b)(iv) *refers to devices that are intended for the diagnosis, treatment, mitigation, or prevention of disease or disorder in human beings or animals*. The specific devices falling under this category may be determined by the Central Government through notification in the Official Gazette, following consultation with the Board. The provided definition lacks precision on the specific instruments employed for diagnostic purposes. Which kind of devices are encompassed under the scope of this definition? These devices refer to tools and medical equipment, namely Electronic Medical devices, which are utilized for diagnostic purposes or are connected to the Internet. The scope of equipment designed for diagnosing patients, whether for internal or external use, is not predetermined.

In Section 3 clause 7 (f), the term "manufacture" in relation to any drug [or cosmetic] includes *any process or part of a process for making, altering, ornamenting, finishing, packing, labelling, breaking up or otherwise treating or adopting any drug [or cosmetic] with a view to its [sale or distribution] but does not include the compounding or dispensing [of any drug, or the packing of any drug or cosmetic,] in the ordinary course of retail business; and "to manufacture" shall be construed accordingly;]*

The provided definition of manufacture lacks an examination or inclusion of the medical device maker or the diagnostic device. The definition mostly centers on the drug's producer only.

In Section 8, covers the standards of quality, in which given the meaning of "*standard quality.*"

(a) in relation to a drug, that the drug complies with the standard set out in [the Second Schedule], and

The phrase establishes a standard solely for the "drug" and does not include any provisions for the "devices" utilized in patient diagnosis.

In Section 8 (b) covers the relation to a cosmetic that the cosmetic complies with such standard as may be prescribed.

Likewise, the established criteria pertain solely to the aesthetic aspect. The absence of a comprehensive discourse pertaining to the gadgets and instruments employed within the healthcare industry has been observed.

Section 18 covers the '*Prohibition of manufacture and sale of certain drugs and cosmetics*.' *This provision of the regulation prohibits the use of any substance categorized as a medication, cosmetic, or medicine that contains any ingredient deemed dangerous or detrimental for use. However, it is imperative to not restrict the usage of medical instruments that may pose harm or emit UV radiation while diagnosing patients, if they do not pose any immediate danger or risk to their well-being or life.*

Section 24 discusses, '*persons bound to disclose the place where drugs or cosmetics are manufactured or kept'. In this Section, it is not obligatory for the maker of the medical equipment to provide information regarding the location of its production. It is feasible for individuals from other countries to readily develop their market presence and engage in the sale of medical devices within India without any obligation or requirement to reveal the country of origin.'*

In Sections 26A and 26B. Discussing the powers of the central government. This analysis only centers on and addresses the dimension of the prohibition imposed on makers of pharmaceuticals and cosmetics in the context of public interest. Section 26B of the document pertains to the authority vested in the Central Government to oversee and control the regulation and production of pharmaceutical substances, among other related activities, with the objective of serving the general welfare. Neither of these laws addresses the aspect of medical device manufacturing. There are currently no restrictions on the utilization of medical technologies that pose potential dangers to individuals in the process of diagnosing patients.

The following are the eight new medical items that are now regulated under the Drugs and Cosmetics Act, 1940:

a. Bone Marrow Cell Separator- Bone marrow cell separator is lab equipment used to isolate cells from bone to blood.

b. X-Ray machine- It is a machine that helps in getting X-rays. It consists of an X-ray detector and an X-ray generator. X-rays are types of

electromagnetic waves. X-ray imaging is a type of imaging that generates pictures of the inside of your body.

c. Dialysis machine- The dialysate is mixed and monitored by the dialysis machine. Dialysate is a fluid that aids in the removal of undesirable waste products from the bloodstream. It also helps in the replenishment of electrolytes and minerals in your body.

d. PET Equipment- PET (polyethylene terephthalate) is the most popular thermoplastic polymer resin of the polyester family and is used in garment fibers, liquid and food containers, thermoforming for manufacturing, and engineering resins in conjunction with glass fiber.

e. Defibrillators- A defibrillator is a machine that delivers a high-energy electric shock to a person who is experiencing cardiac arrest. Defibrillation is the name for this high-energy shock, and it's an important element of attempting to resuscitate someone who's in cardiac arrest.

f. MRI Equipment- Magnetic Resonance Imaging (MRI) is a non-invasive imaging technique that provides precise three-dimensional anatomy pictures.

g. CT Scan Equipment- A computerized tomography (CT) scan combines a sequence of X-ray pictures taken from various angles around your body with computer processing to generate cross-Sectional images (slices) of the bones, blood arteries, and soft tissues within your body.

h. All Implantable Medical Devices- Devices used for any kind of implant such as a dental implant, etc.

The Drugs and Cosmetics Act of 1940 does not include any laws, regulations, or policies pertaining to the eight newly developed medical equipment, namely tools utilized for patient diagnosis. Furthermore, the absence of a paragraph addressing culpability for device failure, or output errors raises the question of accountability in such instances.

B. Drugs and Cosmetics Act as amended in 1964.

The Drugs and Cosmetics Act of 1940 encompasses provisions outlined in Sections 3, 4, 5, 6, 7A, 8, 9B, 10, 12, 16, 17B, 18, 18A, 19, 23, and the substitution of Section 27 and 28 of the Drugs and Cosmetics Act of 1940 has

taken place. Finally, the inclusion of Section 33A and the addition of chapter IV A were implemented.

The primary emphasis in all the revisions of the Drugs and Cosmetics Act 1940 lies in the imposition of severe sanctions specifically targeting drug manufacturers. No punitive measures or penalties are imposed in relation to the production of medical equipment. The change to Section 3 of the Drugs and Cosmetics Act of 1940 pertains to the segment that encompasses the defining component. The term "Ayurvedic" refers to a traditional system of medicine originating from India that focuses on holistic healing and natural remedies. In this context, "the Board means" refers to the designated authority or governing body responsible for overseeing and regulating a particular domain or sector. A "Government Analyst" is an individual employed by the government who is trained and authorized to do scientific analysis and testing of various substances or materials. An "Inspector" is an official appointed by a governing body or organization to ensure compliance with rules, regulations, and standards within a specific industry or field. There is currently no universally accepted definition that encompasses the category of electronic medical devices or medical equipment that are connected to the Internet, as debated in scholarly literature.

C. Drugs and Cosmetics Act as of 2008

The Drug and Cosmetics Act of 1940 underwent amendments in 2008 through the medications and Cosmetics Act, which introduced more rigorous provisions pertaining to penalties associated with the production of counterfeit and contaminated medications. A new Section, namely Section 17E, has been incorporated into the Drugs and Cosmetics Act of 1940, immediately following Section 17D. Section 17E pertains to the elucidation of the term 'Adulterated Cosmetics'. Subsequently, Sections 32B, 33KA, and 33KB were included.

The user's text lacks sufficient information to be rewritten in an academic manner. In summary, the modification to the Drugs and Cosmetics Act of 1940 places significant emphasis on and specifically directs attention to the manufacturing of pharmaceutical substances. The authority to oversee and impose limitations on drug production is vested in the Central government,

particularly where such actions are deemed contrary to the welfare of the general population. Moreover, it is imperative to impose severe penalties on pharmaceutical manufacturers who produce drugs that are contrary to the welfare of the public.

The user's text does not contain any information to rewrite. The Drugs and Cosmetics (Amendment) Act of 2008 does not have any specific definition pertaining to medical devices, which are extensively utilized in the healthcare sector. The regulation of medical devices is necessary due to the transition of healthcare into a technologically driven era.

D. The Drugs Rule 1945

These rules introduced by the Central Government by exercising of the power conferred by [Sections 6(2), 12, 33 and 33(N)] of the Drugs and Cosmetics Act, 1940. The Drugs and Cosmetics Rules, 1945, provide provisions for categorizing drugs into schedules, as well as guidelines for storage, sale, display, and prescription of each category.

In Rule 21 (d) define '*manufacture'*, includes a manufacturer of drugs, who may be a Company or a unit or a body corporate or any other establishment in a country other than India, having its drugs manufacturing facilities duly approved by the National Regulatory Authority of that country, and who also has a free sale approval of the drugs approved by the said authority in the concerned country', and/or in other major countries. The definition provided does not include any reference to the production or manufacturing process of the medical device. This Section mostly pertains to and centers around the production of pharmaceutical substances exclusively. The primary focus of the Drug and Cosmetic Rule of 1945 pertains to many aspects, including the License Authority, Import License, Condition of License, Homoeopathic Medical Practitioner coverage, Registration Certificate, Standard for Import of Drugs, and Controlling Authority.

According to Schedule R1, it is required that the medical equipment adhere to the prevailing Indian Standards established by the Bureau of Indian Standards. In the absence of the Bureau of Indian Standards, adherence to international standards such as those established by the International Organization for Standardization (ISO), International Pharmacopeia Standards, and other

relevant standards is required. If there are no national or international standards applicable, the equipment must adhere to the validated standards set by the maker.

The Drugs and Cosmetics Rule, 1945, specifically the Drugs and Cosmetic (Second Amendment) Rules, 2013, includes the addition of Rule 122. The following regulations outline the necessary conditions that must be met for a clinical study to be deemed sufficient and receive authorization from the governing body to be conducted on human subjects. Moreover, the regulation grants the licensing authority the ability to impose supplementary requirements that must be met for the approval of a particular clinical research, at its discretion. The provision exclusively pertained to drug trials within the context of clinical research. To regulate the matter, the governing body establishes regulations. However, within the context of the medical device trial, there exists a discourse surrounding the topic and its regulatory aspects.

The inclusion of Rule 122 DD in the Drugs and Cosmetics Rule, 1945, also known as the Drug and Cosmetics (Third Amendment) Rules, 2013.

E. Drugs Control Act 1950

This legislation encompasses provisions pertaining to the regulation of the sale, supply, and distribution of pharmaceutical substances. The Drugs Control Act does not encompass or address the regulations and guidelines pertaining to the commercialization of medical devices and their distribution to the intended recipients or the healthcare sector.

F. Drugs, Medical Devices, and Cosmetics Bill, 2022

The Drugs and Cosmetics Act of 1940 is a legislative measure that was passed by the Central Legislative Assembly prior to India's independence. The ongoing process of reviewing and updating laws, including those that have become obsolete, is necessary to address evolving needs and the incorporation of emerging technologies. The government has consistently stressed the importance of reviewing outdated laws and regularly repealing and amending legislation. To achieve this objective, bills are being presented to Parliament. A committee was established to draft the New Drugs, Cosmetics and Medical Devices Bill, in response to the suggestions of the Central Government and

the perceived necessity for comprehensive legislation in this area. In accordance with the suggestions put forth by the Committee. The governmental department responsible for overseeing matters related to public health and the well-being of families, commonly referred to as the Ministry of Health and Family Welfare. The Government of India has put out a draft bill titled "New Drugs, Medical Devices and Cosmetics Bill, 2022" with the aim of aligning with evolving requirements, contemporary circumstances, and advancements in technology.

The primary objective of the Bill is to modify and consolidate the legislation pertaining to the importation, production, distribution, and commercialization of pharmaceuticals, medical devices, and cosmetics. Its purpose is to guarantee the quality, safety, effectiveness, performance, and clinical testing of new drugs, as well as the investigation of investigational medical devices. Additionally, the Bill addresses related matters and any issues that may arise in connection with or because of these activities.

In the definition part, Section 3(v) covers the "investigational medical device" means:

'*a device which does not have a predicate device, or a substantially equivalent device approved earlier by the Central Licensing Authority;*'

The definition of the term "predicate device" is not explicitly provided in this legislation. However, upon examining its literal interpretation, it refers to a medical device that is legally allowed to be sold in the United States and serves as a reference point for evaluating new medical devices seeking approval through the FDA's 510(k) premarket clearance pathway(Deep, 2022). The extent of coverage for investigational medical devices remains unclear. Does this area encompass smart devices, such as IoT-based technological medical devices, or does it only focus on simple Electronic Medical Devices?

The definition of Medical Devices Includes (S.3(zd)):

All devices including an instrument, apparatus, appliance, implant, material or other article, whether used alone or in combination, including a software or an accessory, intended by its manufacturer to be used specially for human beings or animals which does not achieve the primary intended action in or on

human body or animals by any pharmacological or immunological or metabolic means, but which may assist in its intended function by such means for one or more of the specific purposes of:

a. Diagnosis, prevention, monitoring, treatment, or alleviation of any disease or disorder.

b. Diagnosis, monitoring, treatment, alleviation, or assistance for any injury or disability.

c. Investigation, replacement or modification or support of the anatomy or of a physiological process.

d. Supporting or sustaining life.

e. Disinfection of medical devices.

f. Control of conception.

In-vitro diagnostic device, which is a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, equipment, or system, whether used alone or in combination thereof intended to be used for examination and providing information for medical or diagnostic purposes by means of examination of specimens derived from the human bodies or animals.

This definition encompasses all devices that employ software, either independently or in conjunction with software, that are designed for use by individuals. However, it should be noted that the list does not encompass the latest technological products that are produced through the utilization of the Internet of Things (IoT) and Artificial Intelligence (AI) technologies. Healthcare gadgets that use advanced technologies such as artificial intelligence (AI) or the Internet of Things (IoT) are not encompassed within the scope of medical devices as defined in the medical gadgets and Cosmetics Bill of 2022.

Chapter II of the Drugs, Medical Devices, and Cosmetics Bill 2022 delves into the topic of 'Technical Advisory Boards, Drugs Laboratories, Medical Devices Testing Centers, and Consultative Committee'. This Section fails to provide an explanation about the methods employed for evaluating smart or advanced medical equipment. If a smart gadget is introduced into the healthcare market for commercial purposes, and subsequently malfunctions, there is a potential risk to patient safety and well-being.

Standard for imported Drugs and cosmetics:

Chapter III of the Drugs, Medical Devices and Cosmetics Bill 2022 addresses the standard for imported drugs. However, it does not include any provision pertaining to the standard for imported medical devices from outside India. It is worth noting that a significant portion of advanced medical devices in India are imported from the United States and the European Union. Nevertheless, the absence of regulations to standardize these devices and establish quality control measures is evident. Section 27 of the bill addresses the penalty for the death of an individual resulting from the consumption of such drugs. However, there is no mention of penalties for incidents involving medical device failures and any resulting harm to patients or individuals.

Provision related to Import, Manufacture, Sale, Distribution, and Clinical Investigation of Medical Devices:

Chapter VI of the rules encompasses the provisions pertaining to medical devices. This pertains to the regulatory framework governing the manufacturing and distribution of medical devices, as well as the associated consequences for non-compliance with the stipulations outlined in the legislation. Once the maker or importer of medical devices has obtained the necessary license, they are required to file the adverse event report as stipulated in Section 125 (2). Following the Section, medical gadgets are brought into the market and made available for purchase or utilization. If the equipment malfunctions or poses a risk to the patient's well-being. How would the determination of liability be made?

Section 130 pertains to the Prohibition of the import, manufacture, and sale of medical devices. It outlines certain conditions under which manufacturers or importers of medical devices should be prohibited from selling said devices. However, it does not explicitly state that if the manufacturer or importer fails to protect and secure patient data, the device should be prohibited from sale.

If a medical device manufacturer or importer sells a device that, when used by any individual for the diagnosis, treatment, mitigation, or prevention of any disease or disorder, causes bodily harm that qualifies as grievous hurt under Section 320 of the Indian Penal Code (45 of 1860), or is likely to cause such harm or death solely due to the device, they shall be subject to imprisonment

for a period of no less than five years but potentially up to seven years. Additionally, they shall be liable to pay a fine of no less than seven lakh rupees (s.152 (a)). If a medical device has a failure because of hacking or a deliberate attack by a third party, resulting in the device ceasing to function or accurately diagnose a patient, and subsequently leading to the patient's demise, may the medical device manufacturer be held accountable for such an outcome? In this instance, it can be observed that this Section does not offer any substantial elucidation.

G. Indian Medical Council Act, 1956

This legislation addresses issues related to the reconstruction of the Indian Medical Council, the upkeep of an Indian medical registry, and other related subjects. This document encompasses various aspects related to the registration and establishment of medical colleges or institutions. It outlines the qualification criteria necessary for registration, identifies the authorities responsible for issuing licenses, and specifies the terms of office for the president, vice president, and other members. The legislation does not explicitly address the management of medical data or the establishment of regulations pertaining to medical devices. This mostly encompasses the processes of registration and regulation pertaining to medical institutions exclusively.

H. Indian Medical Council (Amendment) Act 1964

The modification to the Indian Medical Council Act of 1956 has additional Sections that pertain to the establishment of minimum criteria for medical education and the regulation of professional behavior. The Indian Medical Council (Amendment) Act of 1964 does not include any provisions or discussions pertaining to the definition or standardization of medical device regulation.

I. Indian Medical Council (Amendment) Act 1993

The Indian Medical Council statute (MCA), 1956, was further revised by this statute itself. Significant modifications can be observed in the subsequent Section 10 of the MCA, accompanied by the introduction of Sections 10A, 10B, and 10C. This encompasses the authorization for the establishment of additional medical colleges, as well as the introduction of new courses of

study, among other related matters. This amendment fails to thoroughly analyze the novel healthcare technologies and their regulatory measures.

J. Indian Medical Council (Amendment) Act, 2001

The Indian Medical Council Act of 1956 is amended by this legislation. There exist two amendments, specifically in Section 13 (a) subsection (3). The proposed amendment suggests the inclusion of the phrase "before such date as the Central Government may, by notification in the Official Gazette, specify after the words "granted by medical institutions outside India". Additionally, the amendment pertains to Section 33, where a new clause (ma) will be inserted after clause (m), '*The modalities for conducting screening tests under sub-Section (4A), and under the proviso to sub-Section (4B), and for issuing eligibility certificate under sub-Section (4B), of Section 13*'. The patient's medical record is not covered by any such change.

K. Indian Medical Council (Professional conduct, Etiquette and Ethics) Regulations, 2002

This regulatory framework encompasses the obligations and roles of physicians in a broad sense. Chapter I of the document addresses Rule 1.3, which pertains to the proper management and upkeep of medical records.

1.3.1 Every physician shall maintain the medical records pertaining to his / her indoor patients for a period of 3 years from the date of commencement of the treatment in a standard proforma laid down by the Medical Council of India and attached as Appendix 3.

1.3.2. If any request is made for medical records either by the patient / authorized attendant or legal authorities involved, the same may be duly acknowledged and documents shall be issued within the period of 72 hours.

1.3.3 A Registered medical practitioner shall maintain a Register of Medical Certificates giving full details of certificates issued. When issuing a medical certificate, he/she shall always enter the identification marks of the patient and keep a copy of the certificate. He/She shall not omit to record the signature and/or thumb mark, address, and at least one identification mark of the patient on the medical certificates or report. The medical certificate shall be prepared as in Appendix 2.

1.3.4 Efforts shall be made to computerize medical records for quick retrieval.

The lack of a universally agreed-upon definition for medical records in relation to patients raises the key question of whether such records encompass solely physical documentation or extend to encompass electronic medical data as well. The lack of clarity arises from the absence of a precise definition for the term "medical record" in the given context. Furthermore, if the medical record of a patient is not furnished to either the guardian or the patient within a span of 72 hours, it raises the question of the party responsible for addressing this issue. In the event of misplacement or theft of stored patient data by a healthcare professional, what are the potential penalties that may be incurred? Regarding any of these matters, this regulation does not provide any explicit guidance or provisions.

L. Indian Medical Council (Amendment) Ordinance, 2016.

The Act provides for the constitution of the Medical Council of India (MCI). The MCI regulates(*The Indian Medical Council (Amendment) Ordinance*, 2016):

i. Standards of medical education.

ii. Permission to start colleges, courses or increase the number of seats.

iii. Registration of doctors,

iv. standards of professional conduct of medical practitioners; etc.

The Ordinance introduces a uniform entrance examination for all medical educational institutions. This would be applicable at the undergraduate and postgraduate level. The Ordinance states that in case a state has not opted for the uniform entrance examination, then the examination will not be applicable at the undergraduate level for the academic year 2016-17. This provision will apply to state government seats in state government and private medical colleges.

The primary emphasis of the Indian Medical Council of India pertains to the establishment and maintenance of standards for medical education. The absence of discourse pertaining to the standardization of patient medical data is evident. This pertains to the mechanisms involved in the storage, processing, and transmission of data between healthcare facilities.

M. Indian Medicine and central council act 1970

The primary objective of this legislation was to establish a Central Council of Indian Medicine and facilitate the establishment and maintenance of a Central Register of Indian Medicine. The act also addresses many related topics. This act primarily centers around the establishment of the central council, the formation of committees, the stipulations of the tenure of office held by authorities, and the acknowledgement of medical credentials. There is a lack of provision, clause, definition, or coverage pertaining to the authorities and committees responsible for regulating medical devices.

N. Medical Termination of Pregnancy Act 1971

The discussed legislation pertains to the cessation of specific pregnancies by duly licensed medical professionals, as well as related and ancillary problems. In Section 3, which pertains to the circumstances in which certified medical practitioners are authorized to terminate pregnancies.

1. In aligning with the terms of this Act, a registered medical practitioner shall not be deemed to have committed any offence under the Indian Penal Code (45 of 1860) or any other applicable legislation if they terminate a pregnancy.
2. In accordance with the stipulations outlined in sub-section (4), a registered medical practitioner has the authority to terminate a pregnancy under the following circumstances: (a) if the duration of the pregnancy is no more than twelve weeks, provided that the medical practitioner is registered, or (b) if the duration of the pregnancy exceeds twelve weeks but does not exceed twenty weeks, provided that at least two registered medical practitioners are involved. Researchers have the opinion, which has been established in good faith, that.
    i. The decision to terminate the pregnancy may be warranted if there is a potential threat to the pregnant woman's life or significant harm to her bodily or mental well-being.
    ii. There exists a significant potential for the kid to experience severe physical or mental impairments, resulting in large handicaps, if it were to be born.

Explanation 1: In cases when a pregnant woman claims that her pregnancy is the result of rape, it is believed that the distress caused by such pregnancy constitutes a significant harm to the mental well-being of the pregnant woman.

Explanation 2: In cases where a pregnancy arises due to the failure of contraceptive measures employed by a married woman or her spouse to control the number of children, it can be inferred that the distress caused by such an unintended pregnancy can be considered a significant harm to the mental well-being of the pregnant woman.

There is a lack of provision or explicit specification that includes any mention of a gadget. The scope of devices covered within the parameters of a given device lacks clarity. The object in question has the potential to serve as either a surgical instrument or an electronic medical device. It is imperative to include a clear and concise definition of any given gadget. In the explanation 2 of Section 3 under the Medical Termination of Pregnancy Act of 1971 pertains to the inadequacy of any contraceptive device. The term any gadget lacks a clear definition under the provisions of this legislation.

O. Medical Termination of Pregnancy Rule, 1975

The rules are hereby established by the Government, in accordance with the authority granted by Section 6 of the Medical Termination of Pregnancy Act, 1971 (34 of 1971). The definition has been expanded to include the term 'location'. Section 4, titled "Approval of Place," and Section 5, titled "Inspection of Place," are thereafter explored in further detail. No clauses or provisions have been included that address the definition of medical devices and their regulation.

P. The Homeopathy Central Council Act 1973

The legislation pertains to the establishment of a Central Council of Homoeopathy and the establishment and management of a Central Register of Homoeopathy, together with related topics. The requirements primarily encompass the construction of a central council, committees, regulations regarding the tenure of office by the authorities, recognition of medical qualifications, and the creation of a central registration for Homoeopathy. There is a lack of any phrase, term, or provision that specifically addresses the

element pertaining to the authorities and committees responsible for regulating medical devices.

Q. Mental Health Act 1987

The legislation in question pertains to the legal aspects surrounding the treatment and care of individuals with mental illness. Its purpose is to enhance the provisions concerning their property, mental healthcare authorities, psychiatric nursing hospitals, and residential facilities. This legislation does not encompass or address any provisions pertaining to medical equipment utilized for the purpose of diagnosing individuals with mental illnesses.

R. Transplantation of Human Organ and Tissue Act, 1994

This regulation primarily focuses on the key provisions pertaining to the transplantation of human organs and tissues. In this regard, it is essential to identify the governing bodies vested with the authority to conduct inspections of hospitals and address patient complaints and grievances. This text aims to elucidate the concepts of organ donation, age limitations, and regulations pertaining to the extraction and transplantation of human organs. The specific instruments and devices utilized in the field of organ transplantation have not been clearly delineated. The topic of medical gadgets utilized in the context of organ transplantation remains unaddressed and unexplored. This inquiry pertains to the types of medical devices that are encompassed within the scope of coverage, as well as the corresponding liabilities associated with those devices.

4.3.2. Rules, Regulation, and the Laws related to Patient Data Protection and the New Medical Devices in the Healthcare

A. Information Technology Act, 2000

In 1996, UN Commission on trade law developed a model law for e-commerce and digital complexity. After this decision, all the other countries took steps to set their own e-commerce laws. The Union Government on 16th December 1999 introduced in Lok Sabha, the much-awaited Cyber

Legislation to establish the legal foundation for electronic commerce and to enable electronic administration in the country. The Information Technology Act was passed on 6th May 2000. The focus of this act is to provide legal recognition for the transaction carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies. It means the IT Act promotes a paper-based method of medical record storage that should be replaced with an electronic mode.

The term "Data Protection" or "Data Privacy" is not utilized in the Preamble Section. The primary focus of this study pertains to the legal recognition of transactions conducted in the realm of internet commerce. The primary objective is to provide the operational framework for the electronic commerce enterprise. The primary objective of implementing the IT Act does not revolve around prioritizing the preservation of data privacy and data protection.

In Section 2(i) defines ***computer***-

A computer is defined as a device or system that utilizes electronic, magnetic, optical, or other high-speed data processing mechanisms to perform logical, arithmetic, and memory operations through the manipulation of electronic, magnetic, or optical impulses. It encompasses all components such as input, output, processing, storage, computer software, and communication facilities that are interconnected or associated with the computer within a computer system or computer network. This definition of a computer does not encompass the inclusion of advanced medical devices such as Internet of Things (IoT) or artificial intelligence (AI)-based technologies that are utilized within the healthcare industry. Additionally, it is important to note that the processing, storage, and transfer of data are distinct functions. Therefore, it is imperative to establish distinct definitions for each of the three entities.

B. The Information Technology (Amendment) Act, 2008

In this amendment, the main goal was to develop and promote the IT industry, regulate e-commerce, facilitate e-governance, and add a Section for the penalties. Insertion of Section 43A that deals with '*compensation for failure*

to protect data' and Section 72A '*Punishment for disclosure of Information in breach of lawful contract'.*

In Section 43A of Information Technology Act 2008:

In cases where a corporate entity possesses, handles, or deals with sensitive personal data or information in a computer resource that it owns, controls, or operates, and demonstrates negligence in the implementation and maintenance of reasonable security practices and procedures, resulting in harm or benefit to any individual, said corporate entity shall be held accountable for compensatory damages. The maximum amount of compensation shall not exceed five crore rupees. The term "body corporate" refers to any type of company, including firms, sole proprietorships, or other associations of individuals involved in commercial or professional endeavors. The subject of sensitive personal data is addressed under Section 43A of the IT Act, as previously mentioned. However, the legislation in question lacks the ability to provide a comprehensive definition of the term "sensitive personal data". The term is utilized within the context of Section 43A in various corporate settings. There is a lack of clarification regarding whether international enterprises are included in the coverage.

Reasonable security practices and procedures means:

The statement pertains to the implementation of security practices and procedures with the intention of safeguarding information from unauthorized access, harm, utilization, alteration, disclosure, or impairment. These practices and procedures are typically outlined in a mutually agreed upon agreement between involved parties or mandated by applicable legislation. In the absence of such an agreement or legislation, the Central Government, in consultation with relevant professional bodies or associations, may prescribe reasonable security practices and procedures. If an organization implements appropriate security measures, and despite this, hackers or attackers manage to breach the stored data, the existing rule fails to address and determine accountability in such cases.

Sensitive personal data or information means:

Such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem

fit. The classification of sensitive personal data falls under the jurisdiction of the central government. Individuals have the authority to include any relevant information or data within the scope of sensitive personal data, as they see appropriate. The scope of sensitive personal data remains ambiguous, as there is a lack of clarity regarding the specific information or data that falls within its purview.

In Section 72 of Information Technology Act 2008:

Unless stated otherwise in this Act or any other currently applicable legislation, it is deemed unlawful for an individual to disclose any electronic record, book, register, correspondence, information, document, or other material to a third party without the consent of the person involved, if said disclosure was obtained through the exercise of powers granted under this Act, its associated rules, or regulations. Violation of this provision may result in a penalty of imprisonment for a period of up to two years, a fine of up to one lakh rupees, or both. Section 72 of the act grants an individual who has been bestowed with authority the ability to obtain entry to electronic records, contingent upon obtaining authorization from the relevant parties. If an unauthorized individual, lacking any authority granted by this legislation, has access to an electronic record and subsequently discloses it to the public. In the given case, the determination of liability is contemplated. In contrast, this area remains devoid of any auditory output.

In Section 72A of Information Technology Act 2008:

72A dealing with the 'Punishment for disclosure of information in breach of lawful contract'. In the healthcare industry, individuals utilize Smart Medical Devices, which necessitate the installation of software on their mobile devices. During the software installation process, a contractual agreement is established between the user and the device maker. In instances where devices experience malfunction or when there is a violation of any provision inside the smart contract. This Section does not encompass the discussion of penalties associated with the violation of smart contracts.

C. The Information Technology Rule 2011

The Information Technology Act of 2000, also referred to as the IT Act, has been updated by the Information Technology (Amendment) Act of 2008.

These legislative measures provide specific regulations pertaining to the privacy and protection of personal and sensitive data under the jurisdiction of India. While the IT Act includes certain Sections that seek to govern the handling of personal data in the digital realm, its main emphasis lies in establishing regulations for information security to safeguard personal and sensitive data in cyberspace. The Central Government has implemented the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, also referred to as "The SPDI Rules," to comply with data protection regulations outlined in the IT Act. The SPDI Rules consist of provisions designed to govern and regulate:

i. The handling of personal data and/or sensitive personal data.

ii. Establishing security protocols and guidelines for the management of Personal Data/Information and/or Sensitive Personal Data/Information(*IT Act & SPDI Rules: Data Protection Regime of India*, 2021).

One significant limitation of the SPDI rule is that it does not apply to a body corporate, such as Body Corporate, if it is situated outside the jurisdiction of India. The current SPDI laws lack explicit clarification regarding their applicability to foreign nationals residing in India. The rules prescribed under the Security and Privacy of Digital Identity (SPDI) framework primarily focus on safeguarding sensitive personal data that is obtained through online channels exclusively. There is a lack of provisions or regulations pertaining to the protection of offline sensitive personal data. The absence of a specialized national regulatory body as stipulated by the SPDI Rules has resulted in inadequate execution of the data protection measures.

D. Personal Data Protection Bill (PDPB)2019

The introduction of the Personal Data Protection Bill, 2019 took place in the Lok Sabha, the lower house of the Indian Parliament, under the auspices of Mr. Ravi Shankar Prasad, the Minister of Electronics, and Information Technology, on December 11, 2019.

In Preamble part of PDPB:

The objective is to establish measures that safeguard the privacy of individuals with regards to their personal data, delineate the handling and utilization of personal data, foster a sense of trust between entities processing personal data

and the individuals concerned, uphold the rights of individuals whose personal data is being processed, establish a framework for organizational and technical measures in data processing, establish regulations for social media intermediaries, address cross-border data transfers, enforce accountability for entities processing personal data, provide remedies for unauthorized and detrimental data processing, and establish a Data Protection Authority of India for the aforementioned purposes and related matters. The primary objective of the Preamble is to establish safeguards for the privacy of individuals, specifically pertaining to personal data. The fundamental issue of the Personal Data Protection Bill (PDPB) 2019 does not revolve around the protection of patient data or the patient's sensitive data. The erosion of trust between patients and doctors can occur when personal data is inadequately maintained or secured.

Definition of Sensitive data in PDPB:

In the definition part, Section 3(36) defines sensitive personal data means such personal data, which may, reveal, be related to, or constitute:

- ***(i)*** *Financial Data.*
- ***(ii)*** *Health Data.*
- ***(iii)*** *Official Identifier.*
- ***(iv)*** *Sex Life.*
- ***(v)*** *Sexual Orientation.*
- ***(vi)*** *Biometric Data.*
- ***(vii)*** *Genetic Data.*
- ***(viii)*** *Transgender Status.*
- ***(ix)*** *Intersex Status.*
- ***(x)*** *Caste or Tribe.*
- ***(xi)*** *Religious or Political Belief or Affiliation; Or*
- ***(xii)*** *Any Other Data Categorized as Sensitive Personal Data Under Section 15.*

Sensitive personal data refers to personal information that is of a delicate or confidential nature. The initial inquiry that emerges from the initial definition pertains to whether all sensitive personal data can be classified as personal data. Furthermore, the aspects that are encompassed or incorporated inside the

term can be understood in a more expansive manner. Section 15 of the Personal Data Protection Bill (PDPB) grants the government the authority to establish supplementary classifications for sensitive data. Furthermore, the inclusion of case or tribe, as well as religious or political belief affiliation, is not obligatory when considering the classification of sensitive personal data. While it is possible that there exists an alternative definition, it is not necessary to include it within the scope of sensitive personal data.

Consent and Processing of Sensitive Data of a Children:

The authority and sectoral regulator are consulted by the Central government to determine and designate personal data as sensitive. To satisfy the legal requirements, it is incumbent upon the government to establish that the data in question poses a substantial danger of harm, while also being accompanied by a reasonable expectation of secrecy, as stipulated in Section 15. To handle the data of minors, the individual or organization responsible for managing the data (referred to as the "data fiduciary") must first confirm the age of the child and acquire approval from their parent or legal guardian. The specific way this consent is obtained will be determined by relevant rules.

Section 16(2) of the Personal Data Protection Bill (PDPB) employs the term 'Personal Data' to refer to the handling of data. The processing of sensitive personal data pertaining to a kid is not mentioned in any context. The Personal Data Protection Bill (PDPB) does not include any explicit provisions regarding the handling of sensitive data pertaining to children. The government possesses the authority to handle confidential information pertaining to minors according to their own set of terms and conditions, without any imposed limitations.

Rights of Data Principal or the patients on the sensitive data:

Chapter V of the Personal Data Protection Bill 2019 pertains to the entitlements granted to individuals, referred to as data principals, in relation to their personal data. The user mentions several rights related to data protection, namely the Right to Confirmation and Access (S.17), Right to Correction and Erasure (S.18), Right to Data Portability (S.19), Right to be Forgotten (S.20), and the General Conditions for the Exercise of Rights in this Chapter (S.21). The rights of the data principle are applicable solely in

instances of personal data processing or storage. The data principle does not explicitly include any rights pertaining to sensitive personal data or patient data. The data principle, referring to the patient, does not possess the right to inquire about the storage, processing, and transfer methods employed by the data fiduciary, which pertains to the healthcare department.

Privacy by Design:

Section 22 of the Personal Data Protection Bill (PDPB) provides an in-depth analysis of the principle of privacy by design. This implies that the technology employed for data processing must adhere to the commercially acknowledged or certified standard as outlined in Section 22(1)(c). However, it is imperative that the data being processed is limited to "personal data" exclusively. It is not necessary for technologies such as AI and IoT, which are employed in the processing of medical data, to adhere to commercially established or certified standards.

Security Safeguard:

In accordance with Section 24, the data fiduciary and data processor are required to establish appropriate security measures, taking into consideration the nature, extent, and objectives of personal data processing, as well as the related risks and potential harm. If sensitive personal data or patient data is being processed, the same measures are followed as outlined in Section 24 of the Personal Data Protection Bill (PDPB). It is important to clarify whether these safeguards are applicable solely to personal data or if they also extend to sensitive personal data and patient data.

Data Protection of Impact Assessment:

In accordance with Section 26(1), when a data fiduciary of substantial importance plans to engage in processing activities involving new technologies or sensitive personal data, such as genetic or biometric data, which may pose a significant risk of harm to data principals, the commencement of such processing shall be contingent upon the completion of a data protection impact assessment, as stipulated in Section 27(3). The Data Protection Assessment lacks the inclusion of data principles and fails to address the potential consequences for patients in the event of a data breach during processing. It does not specify the appropriate legal jurisdiction for

patients to file a lawsuit, nor does it outline the available remedies for affected individuals.

Maintenance of records:

According to Section 26(1) of the legislation, it is required for the Significant Data fiduciary to ensure the maintenance of precise and current records, as stated in Section 28. The specific category of data records being maintained is not mentioned. There appears to be a lack of clarification regarding whether the records in question are personal data or sensitive personal data.

Restriction on transfer of data outside India:

Chapter VII of the Personal Data Protection Bill (PDPB) delves into the laws pertaining to limitations imposed on the transfer of data. There are certain limitations (as outlined in Section 33) regarding the transfer of sensitive personal data and critical personal data outside of India for processing purposes. The governing body sends confidential information beyond the borders of India, while ensuring that this confidential data remains stored inside the territorial boundaries of India. In the process of transferring data from India to foreign nations, instances of data breaches occur. In this scenario, who will bear legal responsibility?

The transmission of data to a foreign country is authorized by the explicit consent of the data principal, as stated in Section 34(1). However, the data principle lacks awareness regarding the potential risks involved in the transfer process, primarily due to the failure of the data fiduciary or the governing authority to disclose such risks.

The Sandbox:

The regulatory body referred to in the Personal Data Protection Bill (PDPB) encourages the development of novel advancements such as Artificial Intelligence, machine learning, and other emerging technologies, with the aim of serving the public's best interests. This is achieved by the establishment of a sandbox, as outlined in Section 40(1) of the bill. To establish or qualify for a sandbox, it is required that a data fiduciary's privacy by design policy be certified by the appropriate authorities as stipulated in sub-Section (3) of Section 22 (40(2)). One notable concern pertains to the absence of a designated space inside the Sandbox application to include information

regarding foreign companies. Is it necessary for international enterprises to establish a regulatory Sandbox? If not, then who bears responsibility for the harm caused by data breaches?

Penalties and compensation:

Chapter X of the Personal Data Protection Bill (PDPB) provides an in-depth analysis of the many consequences that may arise because of failing to comply with data security regulations. If the data fiduciary fails to fulfill the duty of promptly and appropriately addressing a data security breach as outlined in Section 57(1)(a) under Section 25, it will be subject to a penalty that could reach up to five crore rupees or two percent. Wherever it is higher, the whole worldwide turnover of the preceding financial year is considered. This is in accordance with Section 57(3)(a). The primary obstacle pertains to the precision of data, namely the types of data that fall within the scope of a data breach. This Section pertains to confidential personal information.

E. Digital Personal Data Protection Bill, 2022

The primary objective outlined in the initial part of this legislation is to establish a framework for the handling of digital personal data that acknowledges and upholds individuals 'right to safeguard their personal information'. The primary emphasis or consideration lies only on personal data. Within the Section dedicated to definitions, namely in Chapter I, there is an absence of any provision that offers a definition for sensitive data. The provision pertaining to the patient or health data should be addressed. This inquiry pertains to the storage, processing, and transmission of patient data.

Application of the act:

In Section 4, Cleary provides a description stating that the legislation is intended to be applicable to the processing of digital personal data within the geographical boundaries of India. This Section does not address the various considerations related to the processing of sensitive data both within and outside the borders of India. It does not provide any information on this matter.

Transfer of personal data outside India:

The transmission of data outside of India is subject to a clause (S.17) that pertains to the transfer of personal data by a data fiduciary. This transfer can only take place following an assessment by the Central Government.

However, in the context of moving sensitive data outside of India, there is currently no established mechanism, governing entity, or specific legislation in place to regulate such transfers.

Financial Penalty:

The board will levy a financial penalty, as stipulated in Section 25(2), after an assessment of the type and characteristics of personal data that has been compromised due to non-compliance, as outlined in Section 25(2)(b). The occurrence of sensitive or patient data breaches incurs fines imposed by the board. However, it is worth noting that The Digital Data Protection Bill, 2022 does not currently include provisions specifically addressing penalties associated with such breaches.

F. Digital Personal Data Protection (DPDP) Act 2023

This legislation aims to establish a framework for the handling of digital personal data that respects the rights of persons to safeguard their personal information, while also acknowledging the necessity of processing such data for authorized purposes and related matters. The primary emphasis of DPDP lies solely on safeguarding digital personal data.

Definition of Personal Data:

Means any data about an individual who is identifiable by or in relation to such data; (Section 2(t)). The absence of bifurcation or categorization of data is evident, since the act in question encompasses both sensitive and critical material under a single definition of 'Personal Data'. This approach of encompassing all types of data in a unified manner has implications for the security and privacy of user data.

Applicability of the Act:

The scope of this legislation encompasses personal data that is situated within the geographical boundaries of India, and that has been acquired in a digital format or subsequently converted into a digital one. Section 3 of the legislation also encompasses the processing of digital personal data outside of India, if it is connected to the provision of goods and services to individuals within India.

Section 3(c)(i) of the Act stipulates that personal data collected for personal or domestic purposes should not fall within the scope of its application. The

novel aspect is that it will also not be applicable to personal data that has been voluntarily disclosed by the individual to whom it pertains or by any other individual who is legally obligated to do so. This implies that the statute in question does not extend its coverage to personal data that has been voluntarily disclosed on social media platforms or that is subject to other legal provisions.

Processing of Personal Data:

In Section 2(x), "processing" in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organization, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure, or destruction. This definition of processing pertains exclusively to personal data. DPDP Act 2023 does not specify any provisions for the processing of patient data or sensitive data.

The definition parts of this text are insufficient in providing clear definitions for both "sensitive data" and "patient data." The act provides a single definition for "personal data" to encompass all sorts of data, including sensitive, essential, and patient data. To ensure the secure processing of data across various domains, it is important to use distinct security measures. According to certain processing criteria, it is not advisable to process all types of data. In addition, the storage of data necessitates the utilization of various modalities and procedures. The value of important data, such as research and development data, as well as sensitive data like patents and banking information, is immeasurable. An assault or breach has the potential to significantly influence the Gross Domestic Product (GDP) of a country and pose a threat to the well-being of its citizens. To enhance the security of data storage, it is necessary to implement additional security measures. Similarly, when transferring data from one state to another, it is imperative to implement additional security procedures. In general, it is necessary to modify this act by incorporating specific terms that pertain to both sensitive and critical data.

4.3.3 Rules and Regulations pertaining to Patient Medical Data

A. The Clinical Establishments (Registration and Regulation) Act, 2010

The Clinical Establishments Act was implemented by the Central Government with the aim of facilitating the registration and oversight of various facilities and services offered by clinical establishments. The objective of the Act is to facilitate the registration of all clinical establishments in India, so enabling more effective regulation and enforcement of standardized procedures. This is intended to set guidelines for the provision of facilities and services by these establishments, with an emphasis on defining the minimum standards to be upheld. The issue of storing patient medical records and the responsible authority for managing these records and patient data has not been addressed or discussed. The legislation pertains to the registration process of clinical institutions, encompassing diagnostic centers and single-doctor clinics, under all officially recognized systems of medicine, regardless of their affiliation with either the public or private sector, except for those operated by the defense forces. The absence of a policy governing the regulation of electronic medical records for patients is evident.

B. The Clinical Establishments (Central Government) Rules, 2012

The rules are being made by the Central Government in accordance with Section 52 of the Clinical Establishments (Registration and Regulation) Act, 2010 (23 of 2010). In this Section, Rule 9 (iv) will be examined, focusing on the topic of the Electronic Medical Record:

'The clinical establishments shall maintain and provide Electronic Medical Records or Electronic Health Records of every patient as may be determined and issued by the Central Government or the State Government as the case may be, from time to time;'

One significant deficiency that remains is the establishment of a protocol for the retention and storage of patient's medical records. This is the way patient data is saved, processed, and transferred to another healthcare facility. What specific security measures are required for the maintenance of an Electronic Medical Record (EMR) system?

C. Electronic Health Records (EHR) Standard 2016

The primary objective of the health ministry is to implement Electronic Health Records (EHR) to achieve standardization, uniformity, and interoperability in the acquisition, retention, transfer, and utilization of healthcare data across diverse Health Information Technology (IT) platforms. Collaborative endeavors are currently underway among healthcare providers and many stakeholders to facilitate the implementation of these standards(Ministry of Health and Family Welfare, 2017)

In Major Stakeholder list includes:

i. Citizens
ii. Health care providers
iii. Payers, i.e., insurance companies including TPA.
iv. Education, research institutions and investigators
v. Government departments and institutions including law enforcement and courts of law.
vi. Public health agencies and NGOs
vii. Pharmaceutical industry and medical device makers
viii. Telemedicine institutions
ix. Software and hardware vendors

It is important to acknowledge that within the context of an electronic health record system, there exist multiple stakeholders with varying degrees of interest in the acquired data. However, among these stakeholders, only the people and healthcare providers demonstrate an active interest. Consequently, the document will encompass the standards, norms, and laws that are applicable to various entities within the healthcare industry, including healthcare practitioners, healthcare institutions, patients, Independent Software Vendors (ISVs), as well as EHR/EMR System Designers, Manufacturers, Suppliers, and Re-sellers.

Part two of the Electronic Health Record (EHR) standards delves into the examination of the primary stakeholders involved in the implementation of these standards, which includes the medical device manufacturers. The standard prescribed in the Electronic Health Record (EHR) is relevant and enforceable for manufacturers of medical devices. However, it is not clear

whether the same standard of Electronic Health Records is applied to medical equipment manufacturers who are not based in India. Currently, most medical gadgets incorporating technologies such as Artificial Intelligence and the Internet of Things are sourced from foreign countries rather than domestically produced within India. The gadget manufacturer does not provide any established norms or regulations.

The *fourth Section* of the discussion focused on the topics of interoperability and standards. However, there is currently no discourse pertaining to the transfer of patient medical data from India to any foreign nation. The absence of established protocols governing the transfer, storage, and processing of medical data raises concerns regarding the determination of liability in the event of data breaches during the transmission of patient information.

The ownership of electronic medical records (EMRs) is addressed in *Part 7* of the Electronic Health Record Standard. This Section provides a comprehensive list of equipment and technologies utilized for the purpose of electronically accessing, transferring, or receiving patient health information are:

i. Personal computers with internal hard drives used at work, home, or traveling.
ii. External portable hard drives, including iPods and similar devices.
iii. Magnetic tape.
iv. Removable storage devices, such as USB memory sticks, CDs, DVDs, and floppy disks.
v. PDAs and smartphones.
vi. Email.
vii. File transfer.

Within the context of this discussion, there has been an omission in addressing the utilization of sophisticated technologies in the healthcare industry, such as Artificial Intelligence (AI) and Internet of Things (IoT) Medical devices. The Electronic Health Records Standard would not be applicable for that equipment or technology.

D. National Health Policy 2017

The policy aims to achieve optimal health and well-being for individuals of all ages by prioritizing preventive and primitive healthcare approaches in all developmental policies. It also strives to ensure that everyone has equal access to high-quality healthcare services without experiencing financial difficulties as a result.

Rule 23 pertains to the comprehensive examination of the Digital Health Technology Eco-System, which shall now be expounded upon:

'*Recognizing the integral role of technology (eHealth, mHealth, Cloud, Internet of things, wearables, etc.) in healthcare delivery, a National Digital Health Authority (NDHA) will be set up to regulate, develop and deploy digital health across the continuum of care. The policy advocates extensive deployment of digital tools for improving the efficiency and outcome of the healthcare system. The policy aims at an integrated health information system that serves the needs of all stakeholders and improves efficiency, transparency, and citizen experience. Delivery of better health outcomes in terms of access, quality, affordability, lowering of disease burden and efficient monitoring of health entitlements to citizens, is the goal. Establishing federated national health information architecture, to roll-out and link systems across public and private health providers at State and national levels consistent with Metadata and Data Standards (MDDS) & Electronic Health Record (EHR), will be supported by this policy. The policy suggests exploring the use of "Aadhaar" (Unique ID) for identification. Creation of registries (i.e., patients, provider, service, diseases, document, and event) for enhanced public health/big data analytics, creation of health information exchange platform and national health information network, use of National Optical Fiber Network, use of smartphones/tablets for capturing real time data, are key strategies of the National Health Information Architecture*.'

This strategy advocates for the adoption and utilization of innovative healthcare devices that leverage the Internet of Things (IoT) technology and smart wearables. However, ensuring the security of the patient's sensitive data remains the primary obstacle. Furthermore, it is imperative to acknowledge and tackle the security and privacy concerns associated with patient data.

E. Digital Information Security in Healthcare, Act (DISHA, [Draft for Public Consultation]) 2017 and National Electronic Health Authority (NeHA) 2017

The primary objective of the proposed legislation is to establish uniformity and oversight in the procedures pertaining to the acquisition, retention, transfer, and utilization of digital health information. Additionally, it seeks to guarantee the dependability, privacy, confidentiality, and security of such data, along with any other associated and supplementary concerns. The National Electronic Health Authority is vested with the authority to collect digital data for internal purposes (22 1 a (i)), as well as to subsequently transfer health data.

The current discourse lacks a detailed explanation of the data transfer procedure, the circumstances under which data is shared, and the liability in the event of a breach of health data during transmission. Furthermore, if patient data is compromised by an attacker or a third-party intruder, it becomes necessary to determine the allocation of liability after implementing security measures to safeguard the data.

Section 28 of the document delves into the examination of the entitlements possessed by the proprietor of digital health data. This Section encompasses a total of eight rights. However, within the context of these rights, there is no explicit statement, coverage, or discussion on the right of an individual to wipe or delete their personal data at their discretion. Section 33 of the document does not include any explicit information regarding the mechanisms employed for the transfer of data outside the geographical boundaries of India. Additionally, it fails to outline the specific requirements that must be met to facilitate such transfers, as well as the party or parties responsible for ensuring the security and integrity of the data during and after the transfer process, in the event of a breach. Section 33 (2) fails to adequately address the issue of damages and compensation for individuals responsible for breaching digital health data. The individual bears the responsibility of payment, albeit the specific sum remains undetermined. The DISHA act, in its current form, lacks a clear definition of the specific types of breaches that fall within the purview

of Section 38, which pertains to the category of 'severe health data breaches'. This legislation fails to prioritize the emerging technologies employed in the healthcare industry, such as Internet of Things (IoT) devices. Regulation is necessary to govern the collection, processing, and storage of patient data by smart devices, as well as to address potential risks such as device failure and unauthorized access by hackers to sensitive patient information. The determination of culpability in all instances is not addressed by the provisions of this legislation.

F. Medical Device Act 2017

Rule 3: (d) "active medical device" *means a medical device, the operation of which depends on a source of electrical energy or any other source of energy other than the energy generated by human or animal body or gravity. The scope of the definition is limited to devices that are connected or operated utilizing electrical energy. There is currently no existing medical equipment that falls within the classification of an active medical device and is also connected to the internet. In the realm of sophisticated healthcare, a significant portion of healthcare devices are interconnected via the internet, facilitating doctor-patient communication only through online means.*

(zb) "medical device" means, *(A) substances used for in vitro diagnosis and surgical dressings, surgical bandages, surgical staples, surgical sutures, ligatures, blood, and blood component collection bag with or without anticoagulant covered under sub-clause (i).*

The term "medical device" encompasses several instruments and materials utilized in the field of medicine, including in vitro diagnostic tools, as well as surgical dressings, bandages, staples, sutures, ligatures, and blood products. There is a lack of discourse surrounding modern medical gadgets that include technologies such as Artificial Intelligence and the Internet of Things. In contemporary times, smart wireless healthcare gadgets operate by means of the Internet.

Implantable Medical Device-Requirements for regulatory purposes:

Implantable medical device medical device which can only be removed by medical or surgical intervention, and which is intended to:

i. be totally or partially introduced into the human body or a natural orifice, or
ii. replace an epithelial surface or the surface of the eye, and
iii. remain after the procedure for at least 30 days.

The requirement pertaining to Implantable Medical Devices lacks a comprehensive discussion or coverage of devices that include emerging technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI). In the contemporary technological landscape, a multitude of intelligent devices are employed within the realm of healthcare, namely those that are surgically implanted into the human body. Prominent illustrations of such devices are the pacemaker and the cardioverter defibrillator, both of which are designed to operate within the confines of the human heart. The inclusion of these devices is not within the scope of the discussion pertaining to implantable medical devices.

Definition of Manufacturer:

Natural or legal person with responsibility for design and/or manufacture of a medical device with the intention of making the medical device available for use, under his name; whether such a medical device is designed and/or manufactured by that person himself or on his behalf by another person(s). The term “manufacturer” refers to the individual or entity that assumes the responsibility for both the design and production of a medical device, with the explicit purpose of ensuring its availability for use. If a manufacturer from a foreign country is involved and a mistake arises in the design or functionality of the item, it is crucial to determine whether the responsibility lies with the design maker or the hardware maker. The provided definition lacks sufficient clarity when it comes to foreign manufacturers of the equipment.

Definition of Medical device:

Instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination, for human beings, for one or more of the specific medical purposes(s) of:

i. Diagnosis, prevention, monitoring, treatment, or alleviation of disease.
ii. Diagnosis, monitoring, treatment, alleviation of or compensation for an injury.
iii. Investigation, replacement, modification, or support of the anatomy or of a physiological process.
iv. Supporting or sustaining life; control of conception.
v. Disinfection of medical devices; providing information by means of in vitro examination of specimens derived from the human body; and does not achieve its primary intended action by pharmacological, immunological, or metabolic means, in or on the human body, but which may be assisted in its intended function by such means.

The current definition of medical devices lacks comprehensive coverage of modern medical equipment that is interconnected with the internet. The healthcare sector is currently populated with a plethora of intelligent gadgets that leverage artificial intelligence (AI) and Internet of Things (IoT) technology. These intelligent healthcare gadgets are interconnected with the internet, facilitating patients in the online sharing of their data with healthcare professionals.

Medical device file:

For each medical device type or medical device family, the organization shall establish and maintain one or more files either containing or referencing documents generated to demonstrate conformity to the requirement of this International Standard and compliance with applicable regulatory requirements.

The content of the file(s) shall include, but is not limited to:

a) general description of the medical device, intended use/purpose, and labelling, including any instructions for use.
b) specifications for product.
c) specifications or procedures for manufacturing, packaging, storage, handling and distribution.
d) procedures for measuring and monitoring.
e) as appropriate, requirements for installation.
f) as appropriate, procedures for servicing.

The medical device file does not provide information regarding the storage method employed by the device for its data. Where is the sensitive patient data stored and what security measures are utilized to protect the patient data? Furthermore, in the event of the user or patient's demise, it remains uncertain whether the medical device maker retains or erases the patient data.

Control of records:

To demonstrate compliance with regulations and the efficient functioning of the quality management system, it is imperative to uphold and retain appropriate records. The organization is required to establish and maintain documented procedures that outline the necessary controls for the identification, storage, security and integrity, retrieval, retention time, and disposition of documents. The organization is responsible for establishing and executing strategies to safeguard confidential health information stored in records, in compliance with relevant statutory obligations. It is imperative that records be maintained in a manner that ensures their legibility, easy identification, and accessibility for retrieval purposes. Modifications made to a record must be capable of being recognized and traced back to their original form. The organization is required to maintain the records for a minimum duration equivalent to the lifespan of the medical device, as determined by the organization itself, or as mandated by relevant regulatory obligations. However, the retention period must not be shorter than two years from the date of the medical device's release by the organization. The organization possesses the authority to retain the medical device record for the duration of the medical device's lifespan, as stipulated in the control measures. If the user or patient utilizing a medical device were to experience mortality. The deletion of history is contingent upon the device's operational state.

4.4. Quantitative Data Analysis and the Likert Scale 5.0

Legal research relies heavily on quantitative data analysis, which provides a methodical and impartial way to examine data pertinent to legal matters. To get important insights into trends, patterns, and correlations within the legal system. Researchers in this legal study utilize quantitative approaches to study statutes, laws, and court opinions. The study can systematically obtain

data using a variety of quantitative techniques, such as text analysis, questionnaires, and empirical investigations. A pre-made questionnaire using a 5-point Likert scale was used in a particular case study of healthcare data protection and patient privacy. To analyse the current legal framework in India and determine if additional changes are necessary, this survey sought to gather primary data from respondents. The analysis would be based on frameworks in the Indian, US and the EU.

One useful way to get people's opinions and experiences with the legal system is to use questionnaires. The researchers drafted a series of questions with a clear format to ask prospective participants about their experiences with patient data storage practices, opinions on the need for changes to India's current legislative framework, and other relevant topics. Researchers can collect quantitative data on people's awareness of the legal system's protection of patient data and opinions toward certain policies or legislation using the questionnaire approach. As an example, if the researcher is looking at the efficacy of recent legislative change, a questionnaire could ask people about their familiarity with the law and their thoughts on the matter. The study can analyze and quantify the varied opinions within the legal community, the public, or patients using this method, which contributes to evidence-based insights in legal research. It also makes systematic data gathering easier.

4.4.1. Importance of Qualitative Method and the Likert Scale 5.0

Qualitative research methodologies are frequently used by legal academics to explore the complex and multi-faceted elements of legal issues. Recognizing the complexity and interconnectedness of legal concerns with human experiences, and social circumstances, qualitative methodologies were used. When compared to quantitative methods, qualitative research offers a more nuanced picture of the complexities of legal procedures, decisions, and behaviors. When attempting to understand the subjective viewpoints of those involved in the judicial system, this approach shines.

Researchers in the field of law commonly use the Likert scale and more specifically, the 5.0 Likert scale as a reliable quantitative technique for assessing public opinion on issues of legal challenges. Researchers can get a

nuanced and quantified picture of participants 'opinions by using the Likert scale to systematically quantify the degree of agreement or disagreement with claims or propositions. When investigating stakeholder perspectives, expert opinions, or public opinion is vital in legal research, the Likert scale is a useful tool. Specifically, the 5.0 Likert scale provides a well-rounded set of options for respondents to indicate their level of agreement or disagreement, neutrality, or uncertainty.

Level 1 Indicates Strongly Agree.

Level 2 Indicates Agree.

Level 3 Indicates Neutral.

Level 4 Indicates Disagree; or

Level 5 Indicates Strongly Disagree.

The Surveys and questionnaires using the Likert scale help the researcher to collect data on a wide range of legal issues, including public opinion on legislative changes, views on court decisions, and public impressions of legal reforms. Because of its structured design, the Likert scale makes it easy to aggregate and analyse replies, which in turn helps scholars find correlations, patterns, and trends in the field of law. By supplementing qualitative methods with numerical data amenable to statistical analysis, this quantitative approach provides a more all-encompassing grasp of the intricacies of legal matters. For scholars in the field of law who are interested in quantifying and making sense of the complex viewpoints of people who are either directly or indirectly impacted by the judicial system, the Likert scale is a useful and adaptable tool.

4.4.2. Participants for the Questionnaire

A crucial part of a study, especially one involving legal studies, is selecting participants to fill out a questionnaire. To make sure the data is relevant and representative, researchers need to think about the respondent demographics and other personal details. It is prevalent in legal research to specific participant selection to the study's objectives. Data for this study was gathered from a variety of sources, including legal academics, doctors, advocates, and patients. The existing legislative framework for protecting

patient privacy and sensitive data is the primary emphasis of the research. Potential participants may include those who have been directly or indirectly impacted by the problem, as well as those who have encountered difficulties due to the inadequacy of current policies and regulations aimed at protecting patient's data.

4.4.3. Sample Size Determination

For determining the sample size researcher used the Yamen Formula. In the field of legal studies, the work of Japanese statistician Teijiro Yamane known as Yamane's Formula is important, especially for researchers who want to survey or sample a certain community. Finding the sweet spot between precision and practicality, the formula helps researchers choose a suitable sample size.

When time and money are of the essence in legal research, Yamane's Formula is an invaluable instrument. Researchers can gather enough data to make meaningful conclusions without surveying the entire population since it offers a systematic technique to determine sample size.

Considerations like the target confidence level and the allowable margin of error are incorporated into the formula. An effective sample size that reflects the variety within the legal community or among key stakeholders is beneficial for legal research because of the different viewpoints and intricate details that are typically involved.

The trustworthiness and credibility of legal studies are enhanced by Yamane's Formula. Scientists may use this method to modify survey or sample research according to specific legal situations, guaranteeing that the outcomes are representative of the entire legal environment. With the growing use of empirical research methodologies in legal studies, Yamane's Formula provides a practical framework for improving the methodological rigor of research in the discipline.

The adjusted Yamane's formula in equation (4) becomes.

n=N/ (1+N*e^2)

Where n is the sample size to be calculated

- In this case N is the Total Patients size which is 48.3 crore (4800000000)

- In second case N is the Advocate size in India 20 lakh (2000000).
- In Third, N is the size of doctors in India 5 lakh (500000).
- Fourth, N is the size of Legal Academician that is 250000.

E= 0.05 (assumed as 95% level of confidence)

n= 480000000 (1+480000000*0.05^2) (for case one only)

n= 480000000/125601

400 is the sample size chosen.

4.4.4. Distribution of the questionnaire

The researcher has meticulously divided the questionnaire into four distinct Sections to thoroughly investigate different aspects of the subject matter. The **F**irst Section focuses on Demographic Data, aiming to gather significant information on the participant's gender, occupation, and age category. Acquiring this demographic information is vital for comprehending possible disparities in viewpoints among various groups of people.

The **S**econd Section of the questionnaire focuses primarily on matters pertaining to Privacy and the storage of patient information. Its purpose is to collect comprehensive replies that provide insight into participant's perspectives and concerns surrounding the confidentiality of healthcare data. This Section offers a detailed comprehension of how individuals perceive and prioritize privacy considerations in the realm of healthcare information.

The **T**hird segment is devoted to investigating the participant's perspectives on Electronic Medical Record (EMR) systems. The inquiries are likely to inquire about usability, security, and overall perceptions regarding the integration of electronic technologies in the healthcare area. Gaining insight into participants 'perceptions towards EMR systems can provide useful information about the adoption and efficacy of these technologies.

Finally, the **F**ourth Section specifically addresses the integration of the Internet of Things (IoT) and wearables in the Healthcare Sector. This Section is likely to explore the viewpoints, personal encounters, and anticipated

outcomes of participants about the use of IoT devices and wearables in healthcare environments. Examining this region is essential for evaluating the preparedness of folks to adopt technological developments in healthcare and comprehending any reservations or enthusiasm they may possess.

The researcher guarantees a comprehensive examination of demographic aspects, privacy concerns, attitudes towards EMR systems, and opinions on new technologies by categorizing the questionnaire into these four distinct areas. The systematic methodology employed in this study improves its capacity to gather a wide array of viewpoints and perspectives from the participants, so leading to a more thorough and intricate comprehension of the intricate relationship between technology and healthcare in the contemporary setting.

4.4.5. Limitations of the Empirical Study

The questionnaire study presents certain limitations that require cautious examination. The survey's limitation to legal experts, doctors, and advocates may introduce a bias by eliminating opinions from other stakeholders who could offer significant insights into patient data privacy.

Furthermore, the lack of response from several people presents a difficulty, as the motives for their decision not to participate are unreported. The lack of participation in the study introduces a possible bias, which raises concerns regarding the accuracy of the findings and the amount to which the data accurately represents the views of the intended demographic.

This study's emphasis on the complex subject of Privacy and Protection of Patient Sensitive Data suggests that participants who are not familiar with this specialized field may not have a complete understanding of the questions, hence impacting the quality and precision of the collected data.

Questionnaire, which aims to gather demographic information as well as insights into the current healthcare protocols and laws concerning patient data security, can be constrained by participants 'diverse levels of awareness and understanding of these intricate topics.

Ultimately, adopting a nonchalant attitude towards responding to respondents 'questionnaires can result in mistakes and misinterpretations, so undermining

the dependability of the acquired data. These limitations emphasize the necessity for careful analysis of the study's results and emphasize the significance of resolving these restrictions in future research initiatives.

4.4.6. Analysis of the collected Data

i. Demographic Data

The original data acquired for this research was subjected to a rigorous process of data analysis and interpretation, utilizing the powerful Statistical Package for Social Sciences (SPSS). The application of statistical tools, such as frequency distribution, descriptive statistics, and multi-dimensional scaling, was crucial in deriving significant insights from the survey conducted among the respondents. The utilization of these statistical tools was intended to uncover patterns, trends, and relationships that are inherent in the data, so adding to a thorough comprehension of the study subject.

The basic frequency distribution, a fundamental statistical technique, played a crucial role in arranging and displaying empirical evidence in a concise and organized way. By employing this method, it was possible to methodically examine the occurrence of reactions to various factors, thereby illuminating the distribution patterns present in the dataset. The findings obtained from this investigation are concisely presented in the tables, providing a graphical depiction of the empirical data.

In general, the utilization of statistical methods allowed for a thorough and unbiased analysis of the gathered data, enabling the research team to obtain valuable insights and make sound conclusions. Employing a methodical approach to analysing data improves the trustworthiness and dependability of the research results, hence strengthening the overall integrity of the study.

- The study aimed to include a total of 400 people in the sample, ensuring a comprehensive representation. Nevertheless, the researcher obtained feedback from 390 participants after distributing the survey. The demographic breakdown of the participants, as shown in Table 4.1, reveals that out of the 390 responses, 191 identified as female, 197 as male, and 2 persons chose not to declare their gender. To offer a comprehensive analysis, it is crucial to consider the percentage distribution of various gender

categories in respect to the overall number of participants. The data indicates that 49% of the participants are female, 50.5% are male, and 0.5% opted not to disclose their gender. The percentage split provides vital insights into the gender representation in the study, allowing for a more detailed understanding of the participant demographics and adding to the overall interpretation of the research findings.

Q1		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Woman	191	49.0	49.0	49.0
	Man	197	50.5	50.5	99.5
	Prefer not to say	2	.5	.5	100.0
	Total	390	100.0	100.0	

Table 4.1 Representation of Gender

- The researcher systematically allocated the questionnaire set among targeted stakeholders to guarantee a varied and inclusive sample. The examination of participation, as depicted in Table 4.2, elucidates the involvement of various stakeholder groups. Out of all the participants, 5.1% were doctors, 10.5% were advocates, a significant 25.9% were legal scholars, and the majority of 58.5% fell into the "Patients" group. This distribution enables a detailed analysis of the perspectives collected, highlighting significant input from legal scholars and a varied group of professionals classified as "Patients". Incorporating a range of stakeholders improves the thoroughness of the study, allowing for a more comprehensive investigation of the research problem from the perspectives of multiple participant groups.

Q2		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Advocate	41	10.5	10.5	10.5
	Legal Academician	101	25.9	25.9	36.4
	Doctors	20	5.1	5.1	41.5

	Patients	228	58.5	58.5	100.0
	Total	390	100.0	100.0	

Table 4.2 Participants of different stakeholders

- In Table 4.3, depicts the distribution of ages among the participants in this study uncovers valuable and enlightening trends. Out of all the participants, just 1% belong to the age group below 18, whereas those above 36 make up a comparatively small proportion of 3.8%. A considerable 55.4% of responders are between the ages of 19 and 25. In addition, the age group of 26-30 accounts for a significant 28.5%, while those aged 31-35 represent 11.3%. The distribution highlights the prevalence of participants in the 19-25 age group, demonstrating a significant representation of younger adults in the study. The high occurrence of individuals in this age group indicates that the perspectives and opinions collected are especially representative of the views of this demographic, offering significant insights into the thoughts and attitudes of the younger cohort on the subjects being studied.

Q3		**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	<18	4	1.0	1.0	1.0
	19-25	216	55.4	55.4	56.4
	26-30	111	28.5	28.5	84.9
	31-35	44	11.3	11.3	96.2
	36<	15	3.8	3.8	100.0
	Total	390	100.0	100.0	

Table 4.3 Distribution of Age Group

ii. Privacy and Patient-Privacy information storage Related question

- In the research, participants were surveyed about privacy-related legislation. A thorough examination of their responses reveals important patterns. Significantly, 33.3% of participants strongly agreed with the presence of laws prior to the year 2000. Furthermore, a significant 39.7% expressed concurrence with this viewpoint, constituting the prevailing sentiment.

Meanwhile, 25.4% of individuals held a neutral position about the existence of such legislation (Table 4.4). The distribution of replies highlights a significant unanimity among the participants, with a substantial number recognizing the lack of privacy legislation prior to the year 2000. These findings provide detailed and subtle insights into the participants' perceptions and comprehension of the historical legal framework that governs privacy problems.

Q4		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	130	33.3	33.3	33.3
	Agree	155	39.7	39.7	73.1
	Neutral	99	25.4	25.4	98.5
	Disagree	4	1.0	1.0	99.5
	Strongly Disagree	2	.5	.5	100.0
	Total	390	100.0	100.0	

Table 4.4 Participants responses in India before 2000s that protect privacy are not adequate.

- The SPSS analysis of the question "I believe privacy within the family is important" provides insights into participants 'viewpoints on the significance of privacy within the family in Table 4.5. Among the respondents, a significant 42.6% strongly agree on the importance of privacy inside the family, suggesting a prevailing view among the majority. In addition, 41.8% of respondents agreed, resulting in a total of 84.4% who confirmed the significance of maintaining privacy inside the family. Approximately 13.3% of individuals held a neutral position on the topic, indicating a wide range of viewpoints. In contrast, a lesser proportion of individuals, namely 2.3%, held a contrary opinion to the statement, but only 0.5% expressed a strong opposition. This extensive analysis offers useful insights into the consensus and divergences among participants' attitudes regarding the significance of privacy within the family.

Q5		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	166	42.6	42.6	42.6
	Agree	163	41.8	41.8	84.4
	Neutral	52	13.3	13.3	97.7
	Disagree	9	2.3	2.3	100.0
	Total	390	100.0	100.0	

Table 4.5 Participants responses with respect to Privacy within the family

- The researcher's study, "I believe privacy within the relationship is important," offers a comprehensive insight into participants 'viewpoints regarding the significance of privacy in relationships. Almost half (49.2%) of the participants rated the importance of privacy within relationships as high, reflecting a widespread conviction in its significance. In addition, 36.4% of respondents indicated a moderate level of importance with a rating of 2, resulting in a total of 85.6% who acknowledge the significance of maintaining privacy in relationships to some extent (as shown in Table 4.6). 10.8% of respondents gave a grade of 3, indicating a range of viewpoints on the issue. Merely 3.1% of the participants gave a rating of 4, denoting a relatively low level of importance. Furthermore, a mere 0.5% assigned the lowest grade of 5, showing a lack of significance placed on privacy within relationships. This thorough investigation offers useful insights into the varied levels of significance assigned to relationship privacy among the participants.

Q6		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	192	49.2	49.2	49.2
	2	142	36.4	36.4	85.6
	3	42	10.8	10.8	96.4
	4	12	3.1	3.1	99.5
	5	2	.5	.5	100.0

	Total	390	100.0	100.0	

Table 4.6 Participants responses with respect to privacy within the relationship

- The study of participants responses to the statement "I believe privacy within marriage is important" reveals different perspectives on the significance of marital privacy. A substantial 40.0% of respondents gave the highest importance rating of 1, indicating a prevailing belief in the importance of privacy in marriage. Furthermore, 36.7% of participants expressed a moderately high level of importance with a rating of 2, resulting in a combined 76.7% who recognized the significance of marital privacy illustrated in Table 4.7. Notably, 15.4% assigned a rating of 3, indicating a moderate level of importance, while 6.9% assigned a rating of 4, suggesting a lower level of importance. Only a minimal 1.0% assigned the lowest rating of 5, indicating that marital privacy is not crucial to them. This detailed analysis offers a comprehensive understanding of the varying degrees of importance placed on privacy within the context of marriage among the study participants.

Q7		**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	1	156	40.0	40.0	40.0
	2	143	36.7	36.7	76.7
	3	60	15.4	15.4	92.1
	4	27	6.9	6.9	99.0
	5	4	1.0	1.0	100.0
	Total	390	100.0	100.0	

Table 4.7 Participants responses related to privacy within marriage.

- The opinions that are generally held on the importance of personal space privacy are revealed by the responses to the phrase, "I believe privacy within an individual's personal space is important." A significant 55.6% of participants gave the highest rating of 1, suggesting a broad conviction in the utmost significance of privacy in one's personal domain. Furthermore, 38.2% of the participants indicated a relatively high level of importance with a rating

of 2, resulting in a combined 93.8% who recognized the value of personal space privacy. Only a small fraction, specifically 5.6%, gave a grade of 3, indicating a modest level of importance. Significantly, a mere 0.5% were given a rating of 4, suggesting a relatively low level of significance (Table 4.8). This analysis offers a detailed examination that allows for a thorough comprehension of the different levels of significance attributed to privacy inside an individual's personal sphere among the participants of the study.

Q8		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	217	55.6	55.6	55.6
	2	149	38.2	38.2	93.8
	3	22	5.6	5.6	99.5
	4	2	.5	.5	100.0
	Total	390	100.0	100.0	

Table 4.8 Participants responses related to privacy within an individual's personal space.

- The evaluation of those responding to the statement "I believe privacy of patient records is important," as displayed in Table 4.9, unveils the perceived significance attributed to protecting the privacy of patient information. Approximately two-thirds (66.4%) of participants gave the maximum relevance grade of 1, indicating an agreement among the majority regarding the crucial significance of maintaining the privacy of patient records. In addition, 25.4% of the participants indicated a relatively high level of relevance with a rating of 2, adding to a total of 91.8% who recognized the significance of safeguarding patient records. Only 5.9% of respondents rated the importance level as 3, indicating a moderate level of relevance. Additionally, a mere 1.8% awarded a grade of 4, reflecting a lower degree of importance. The analysis highlights the extensive acknowledgment of the utmost significance of upholding privacy in patient records among the survey participants.

Q9	Frequency	Percent	Valid Percent	Cumulative Percent

Valid	1	259	66.4	66.4	66.4
	2	99	25.4	25.4	91.8
	3	23	5.9	5.9	97.7
	4	7	1.8	1.8	99.5
	5	2	.5	.5	100.0
	Total	390	100.0	100.0	

Table 4.9 Participants responses related to privacy of patient records.

- The examination of the feedback regarding the assertion "There is no distinct legislation that addresses Patient Privacy," as displayed in Table 4.10, exposes a variety of viewpoints among the participants. Approximately 24.1% of the participants strongly concur that there is a notable absence of precise laws concerning the protection of patient confidentiality. Furthermore, a significant proportion of 46.4% concur, signifying a considerable shared conviction regarding the insufficiency of current legislation in this field. Conversely, 18.2% maintain a neutral position, indicating a degree of uncertainty or absence of agreement. In addition, 9.7% have a contrary view, whereas 1.5% firmly hold a contrary view, indicating a range of perspectives among the participants. This detailed investigation highlights the intricate nature of beliefs surrounding the current legal structure for maintaining patient confidentiality.

Q10		**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	1	94	24.1	24.1	24.1
	2	181	46.4	46.4	70.5
	3	71	18.2	18.2	88.7
	4	38	9.7	9.7	98.5
	5	6	1.5	1.5	100.0
	Total	390	100.0	100.0	

Table 4.10 Participants responses for the distinct legislation that addresses Patient Privacy

- The examination of the response to the assertion "The Indian healthcare industry stores or retains patient information using a Paper-Based Method,"

as depicted in Table 4.11, offers valuable insights into current perspectives. A significant proportion of participants, specifically 12.6%, strongly agree with the statement, demonstrating a major reliance on paper-based procedures in the healthcare industry. In addition, 44.4% of respondents agree, demonstrating a significant communal recognition of the widespread use of paper-based storage methods. Approximately 29.5% of individuals maintain a neutral position, indicating a group of respondents who neither affirm nor reject the prevailing reliance on paper. In addition, 12.6% express disagreement, questioning the idea, while a mere 1.0% strongly disagree with the statement. The wide array of comments highlights the varying viewpoints on the storage techniques used in the Indian healthcare industry.

Q11		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	49	12.6	12.6	12.6
	2	173	44.4	44.4	56.9
	3	115	29.5	29.5	86.4
	4	49	12.6	12.6	99.0
	5	4	1.0	1.0	100.0
	Total	390	100.0	100.0	

Table 4.11 Participants responses that Indian healthcare industry stores or retains patient information using a Paper-Based Method

- An analysis of the outcomes to the statement “There are rules or regulations in India that exist to safeguard paper-based medical records,” as delineated in Table 4.12, uncovers varied viewpoints on the regulatory structure. A significant proportion of individuals, around 12.3%, strongly believe that rules or regulations are in place to protect paper-based medical records. Furthermore, 45.4% of individuals indicate their agreement, demonstrating a significant collective recognition of the presence of restrictions in this situation. Approximately 35.1% of individuals hold a neutral perspective, indicating a group of respondents who neither affirm nor negate the presence of regulations. In addition, 6.2% express disagreement, questioning the idea,

while a mere 1.0% strongly disagree with the statement. The assortment of comments demonstrates the diverse viewpoints on the regulatory framework around paper-based medical records in India.

Q12		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	48	12.3	12.3	12.3
	2	177	45.4	45.4	57.7
	3	137	35.1	35.1	92.8
	4	24	6.2	6.2	99.0
	5	4	1.0	1.0	100.0
	Total	390	100.0	100.0	

Table 4.12 Participants responses on 'there are rules or regulations in India that exist to safeguard paper-based medical records.'

- A statement "There is a need to change the traditional medical record system," as displayed in Table 4.13, demonstrates a wide range of perspectives regarding the imperative nature of reform in the medical record system. Approximately 38.7% of participants strongly agree that there is an urgent need for change, highlighting a significant consensus on the importance of shifting from traditional medical record procedures. Furthermore, 40.0% of individuals concur, so strengthening the prevailing feeling in support of a transition in the current system. Approximately 13.3% of respondents hold a neutral position, meaning that they neither strongly agree nor disagree. In addition, 6.4% express disagreement, questioning the apparent necessity for change, while a mere 1.5% strongly disagree with the statement. The range of reactions highlights the diverse viewpoints on the need to overhaul the conventional medical record system.

Q13		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	151	38.7	38.7	38.7
	2	156	40.0	40.0	78.7
	3	52	13.3	13.3	92.1

	4	25	6.4	6.4	98.5
	5	6	1.5	1.5	100.0
	Total	390	100.0	100.0	

Table 4.13 Participants responses on 'the need to change the traditional medical record system.'

- An analysis of the responses to the statement "There is a possibility of losing records in the paper-based medical record," as shown in Table 4.14, uncovers noteworthy apprehensions regarding the susceptibility of paper-based medical records. Almost half of the participants, at 47.9%, strongly support the idea, indicating a common belief that paper-based records carry a significant danger of being lost. Furthermore, 41.3% of individuals agree with this issue, which further supports the widely recognized acknowledgement of the possibility of data loss in such a system. 9.2% of the respondents hold a neutral view, indicating a distinct subgroup that neither strongly agree nor disagree. In addition, a small proportion, namely 1.0%, indicates a disagreement with the statement, indicating a difference in opinion regarding the probability of record loss. The variety of responses highlights the perceived dangers linked to the preservation of medical records in a paper-based system.

Q14		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	187	47.9	47.9	47.9
	2	161	41.3	41.3	89.2
	3	36	9.2	9.2	98.5
	4	4	1.0	1.0	99.5
	5	2	.5	.5	100.0
	Total	390	100.0	100.0	

Table 4.14 Participants responses on 'There is a possibility of losing records in the paper-based medical record.'

- Table 4.15 represents the analysis of responses to the statement "Protecting patient privacy is the responsibility of the government," indicates different viewpoints regarding the government's involvement in protecting patient

privacy. 44.9% of participants strongly agree that it is the government's responsibility to preserve patient privacy. The prevailing sentiment among responders highlights the government's critical responsibility in maintaining the confidentiality and security of patient information. Furthermore, 32.8% of respondents concur with this viewpoint, providing additional evidence for the idea that a significant proportion of participant's advocate for the government's active role in protecting patient confidentiality. A minority, comprising 12.8% of the respondents, holds a neutral position on the subject, indicating a group of individuals who neither strongly agree nor disagree with the statement. In addition, 9.0% of participants hold a differing viewpoint, highlighting a variety of opinions regarding the level of responsibility the government should have in safeguarding patient privacy. The data highlights the different viewpoints regarding the government's involvement in addressing this crucial issue of healthcare.

Q15		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	175	44.9	44.9	44.9
	2	128	32.8	32.8	77.7
	3	50	12.8	12.8	90.5
	4	35	9.0	9.0	99.5
	5	2	.5	.5	100.0
	Total	390	100.0	100.0	

Table 4.15 Participants responses on 'Protecting patient privacy is the responsibility of the government.'

- Insights into the opinions around patients 'legal options in the case of a data breach are provided by the examination of responses to the statement, "If a patient's information is breached, they have the right to sue the government," as shown in Table 4.16. Approximately one-third of the participants, namely 32.8%, firmly believe that patients possess the entitlement to legally pursue the government in the event of information breaches. This signifies a significant approval of the notion that individuals should have lawful means to pursue when their privacy is violated. Furthermore, 42.1% of individuals

concur with this viewpoint, so strengthening the notion that pursuing legal measures against the government is a legitimate recourse in such situations. 15.1% of respondents hold a neutral position on the issue, indicating a subgroup that neither strongly agrees nor disagrees with the statement. In addition, 9.0% of participant's express disagreement with the idea, suggesting a difference in view on the level of legal action that patients can take against the government in case of a data breach. The data emphasizes the diverse perspectives regarding the legal consequences of patient information breaches and the possible recourse patients have against the government.

Q16		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	128	32.8	33.2	33.2
	2	164	42.1	42.5	75.6
	3	59	15.1	15.3	90.9
	4	35	9.0	9.1	100.0
	Total	386	99.0	100.0	
Missing	System	4	1.0		
Total		390	100.0		

Table 4.16 Participants responses on 'The right of patients to sue government in case of data breach.'

- The study of the feedback received for the statement "If a medical record (in paper format) is lost, there are remedies available to the person affected," as displayed in Table 4.17, provides insights into the perceptions concerning the accessibility of solutions for those impacted by the loss of medical data. Approximately 16.9% of participants hold a strong belief that victims have effective solutions in the event of a loss of paper-based medical records. This implies a substantial proportion of respondents who strongly believe in the presence of lawful or procedural remedies for those impacted. Moreover, 37.9% of individuals agree with this viewpoint, which further supports the idea that a significant portion recognizes the existence of solutions for victims

in these situations. An additional 32.8% of participants remain impartial on the matter, indicating confusion or a lack of agreement regarding the effectiveness of solutions. In addition, 10.3% of participant's express dissent towards the idea, suggesting that there is a group of respondents who believe that there are not enough solutions for victims of medical record loss. The data highlights the range of viewpoints regarding the efficacy of current efforts to mitigate the effects of losing paper-based medical records, as well as the various levels of confidence in the available solutions.

Q17		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	66	16.9	16.9	16.9
	2	148	37.9	37.9	54.9
	3	128	32.8	32.8	87.7
	4	40	10.3	10.3	97.9
	5	8	2.1	2.1	100.0
	Total	390	100.0	100.0	

Table 4.17 Participants responses on 'If a medical record (in paper format) is lost, there are remedies available to the person affected.'

iii. Electronic Medical Record (EMR) system

- An understanding of participants 'opinions of the importance of technology advancement in the healthcare sector may be gained from the analysis of replies to the statement, "There is a need for the upgradation of technologies in the healthcare system," as shown in Table 4.18. A substantial majority of participants, accounting for 55.6%, strongly support the proposal, underscoring a general recognition of the urgent requirement for technological advancement. Furthermore, an extra 35.1% of participants concur, hence strengthening the consensus on the significance of promoting healthcare innovations. 7.2% of the respondents hold a neutral position on the subject, suggesting a group of individuals who neither strongly agree nor disagree with the statement. In addition, a small fraction of participants

(1.5%) holds a contrary view, indicating a slight disagreement over the importance of technological advancements in the healthcare system. The aggregated data highlights the general consensus among participants who support the improvement of healthcare technologies, indicating a common belief in the beneficial effects that such innovations could have on the overall efficiency and effectiveness of healthcare services.

Q18		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	217	55.6	55.6	55.6
	2	137	35.1	35.1	90.8
	3	28	7.2	7.2	97.9
	4	2	.5	.5	98.5
	5	6	1.5	1.5	100.0
	Total	390	100.0	100.0	

Table 4.18 Participants responses on need of upgradation of technology in the healthcare

- Table 4.19 illustrates the frequency distribution and percentage analysis about the perceived necessity of implementing the Electronic Medical Record (EMR) system in India. The table classifies replies into five levels (1 to 5), which indicate different levels of agreement or urgency in relation to the implementation of EMR systems.

  The study shows that 44.1% of the respondents belong to the category labeled '1', which indicates a strong consensus or high frequency of those who believe that there is a crucial necessity for the installation of EMR systems. This discovery emphasizes a substantial amount of backing for the incorporation of electronic medical records in the healthcare environment of India. The frequency of 40.8% corresponds to the second-highest level, which is labelled as '2'. These responders have a noticeable, if slightly less forceful, position in comparison to the first category. The combined number for the initial two tiers totals 84.9%, indicating a significant majority in support of implementing EMR. The proportion of responses at Level '3'is

13.8%, showing a considerable level of agreement regarding the necessity of EMR systems. Although this organization is very tiny, it still adds to the general agreement to use electronic medical records in India. Levels 4 and 5 collectively represent a small proportion, specifically 1.3% and 1.0%, respectively. The levels indicate a small group of respondents that either have doubts regarding the importance of adopting EMR systems (level '4') or show a lack of agreement (level '5'). To summarize, the data from Table 19 highlights a significant and widespread recognition among respondents on the necessity of implementing EMR systems in India. Most respondents demonstrate a high level of agreement, indicating significant endorsement for the implementation of electronic medical records to improve healthcare procedures in the country.

Q19		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	172	44.1	44.1	44.1
	2	159	40.8	40.8	84.9
	3	54	13.8	13.8	98.7
	4	1	.3	.3	99.0
	5	4	1.0	1.0	100.0
	Total	390	100.0	100.0	

Table 4.19 Participants responses on implementing EMR system in the healthcare sector.

- Table 4.20 provides an examination of the responses regarding the storage of patient data in a cloud system inside the Electronic Medical Record (EMR) framework. The table classifies participants into four groups Strongly Agree, Agree, Neutral, and Disagree representing different levels of approval or objection to the idea of using cloud services for keeping patient data.

  The data analysis indicates that a significant proportion of respondents, up to 31.3%, aligns with the 'Strongly Agree' category. This organization unequivocally supports the concept of keeping patient data in the cloud as an

integral component of the Electronic Medical Record (EMR) system. The proportion indicates a substantial degree of enthusiasm and confidence among these participants regarding the advantages and practicality of using cloud technology for the management of medical records. The 'Agree' category has the highest frequency, accounting for 45.4% of the observations. This suggests that a significant majority of respondents have a favorable attitude towards using cloud services to store patient data. Although not as strongly expressed as the 'Strongly Agree' group, this category nevertheless indicates a broad acceptance and endorsement of the integration of cloud technologies in the EMR infrastructure. The 'Neutral' category accounts for 19.5% of responses, signifying a significant portion of those who neither strongly endorse nor reject the concept of putting patient data in the cloud. These individuals may have doubts or may be apathetic to the concept, indicating a level of ambivalence or uncertainty regarding the utilization of cloud technologies in EMR. The 'Disagree' category comprises the smallest group, accounting for 3.8% of the total. This organization strongly opposes the idea of keeping patient data in a cloud system as part of the Electronic Medical Record (EMR). Although the percentage is very small, it nonetheless emphasizes a minority of respondents who harbor misgivings or concerns regarding this specific component of EMR deployment. To summarize, the data from Table 20 reveals a wide array of attitudes among respondents about the storage of patient data in a cloud system within the context of EMR adoption. Although there is a significant majority in support of using cloud technology, a considerable portion voices concerns or remains impartial regarding this element of managing electronic medical records.

Q20		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	122	31.3	31.3	31.3
	2	177	45.4	45.4	76.7
	3	76	19.5	19.5	96.2
	4	15	3.8	3.8	100.0
	Total	390	100.0	100.0	

Table 4.20 Participants responses on the EMR patient's data stored in Cloud System

- A substantial majority of respondents, according to Table 4.21 analysis, had positive opinions about the security of Electronic Medical Record (EMR) systems for protecting patient privacy and security. More precisely, 73.6% of the participants express either a strong agreement (31.5%) or agreement (42.1%) about the ability of EMR systems to securely protect patient information. This indicates a prevailing trust in the efficiency of EMR systems in upholding the privacy and protection of sensitive medical information. Although a significant percentage (18.5%) remains neutral, neither strongly agreeing nor disagreeing, a minority (6.9%) holds the viewpoint that EMR systems are not a secure method for safeguarding patient data. In addition, a mere 1.0% vehemently disagrees with the statement. Overall, most respondents exhibit a favorable impression, endorsing the idea that EMR systems are a reliable means of safeguarding patient data with confidentiality. The research indicates that the majority of individuals have confidence in the security precautions applied in EMR systems, whereas a minority have concerns or remain impartial on this matter.

Q21		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	123	31.5	31.5	31.5
	2	164	42.1	42.1	73.6
	3	72	18.5	18.5	92.1
	4	27	6.9	6.9	99.0
	5	4	1.0	1.0	100.0
	Total	390	100.0	100.0	

Table 4.21 Participants opinion on the security of the EMR system for protecting patient data.

- The analysis of Table 4.22 presents the viewpoints of participants on the presence of a legal structure in India for the implementation and oversight of the Electronic Medical Record (EMR) system. 56.2% of the participants, a

majority, either strongly agree (17.9%) or agree (38.2%) that there is a legislative framework in place. The respondent's strong approval and endorsement for the implementation and control of EMR systems through legal methods is evident. Approximately 35.1% of the participants have a neutral position, indicating ambiguity or a lack of information regarding the presence of a legislative framework for EMR systems in India. Conversely, a smaller nevertheless significant faction (7.2%) holds a dissenting view about the implementation of these regulations, indicating a degree of doubt or opposition towards the notion that legislative measures are now enforced. Merely a small fraction (1.5%) vehemently opposes the claim that there exists a legislative framework for the implementation and oversight of EMR systems in India. This indicates a distinct subset of participants who strongly oppose the idea of current legislative measures in this situation. Finally, the data from Table 22 reveals a diverse viewpoint among respondents concerning the legal structure for EMR systems in India. Although most people recognize and endorse the concept, a significant portion expresses doubt or disagreement with the claim, emphasizing the necessity for increased understanding and explanation of the regulatory framework for implementing EMR in the country.

Q22		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	70	17.9	17.9	17.9
	2	149	38.2	38.2	56.2
	3	137	35.1	35.1	91.3
	4	28	7.2	7.2	98.5
	5	6	1.5	1.5	100.0
	Total	390	100.0	100.0	

Table 4.22 Participants responses on 'the existing legal system of India for the implementation and oversight of the Electronic Medical Record (EMR) system'

- Table 4.23 analysis indicates a distinct consensus among respondents regarding the imperative nature of obtaining patient or guardian consent

while transferring Electronic Medical Records (EMR) between hospitals in India. 82.6% of participants, consisting of a significant majority, either strongly agree (35.9%) or agrees (46.7%) that gaining agreement is an essential stage in the process of transmitting EMR. Respondents demonstrate a robust acknowledgment of the significance of upholding patient privacy and obtaining consent when exchanging medical information between various healthcare establishments. Approximately 16.4% of participants have a neutral position, indicating a certain level of uncertainty or absence of a strong opinion on the subject. Conversely, a minuscule proportion (.3%) holds a dissenting view regarding the necessity of obtaining consent from patients or guardians for the transfer of electronic medical records (EMR), with just a small fraction (.8%) expressing severe disagreement. The low disagreement percentages highlight the strong consensus that consent is a necessary component in the transmission of EMR data between hospitals.

Q23		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	140	35.9	35.9	35.9
	2	182	46.7	46.7	82.6
	3	64	16.4	16.4	99.0
	4	1	.3	.3	99.2
	5	3	.8	.8	100.0
	Total	390	100.0	100.0	

Table 4.23 Participants responses on obtaining patient or guardian consent while transferring Electronic Medical Records (EMR) between hospitals in India

- The examination of Table 24 presents the viewpoints of participants concerning the government's position on authorizing the global transmission of Indian patients 'Electronic Medical Records (EMR) without doing security procedure assessments. The data reveals a multitude of perspectives among the participants. Approximately half, specifically 50.3%, of the respondents either strongly agree (13.8%) or agree (36.4%) that the government allows international EMR transfers without conducting security protocol reviews.

These findings indicate a notable degree of apprehension or doubt among participants regarding the supervision of security protocols in the global exchange of patient information. Approximately 31.0% of respondents had a neutral posture, suggesting that a significant portion of them may not have a clear opinion or are uncertain about the government's position on this topic. In contrast, 17.2% of individuals hold a different opinion regarding the government's allowance of international EMR transfers without undergoing security procedural review. This indicates that a small number of participants hold the belief that there are probably security measures in effect for international electronic medical record transfers. A minute proportion (1.5%) expresses strong dissent towards the statement, signifying a fraction of participants who vehemently oppose the notion that the government permits international EMR transfers without thoroughly examining security protocols.

Q24		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	54	13.8	13.8	13.8
	2	142	36.4	36.4	50.3
	3	121	31.0	31.0	81.3
	4	67	17.2	17.2	98.5
	5	6	1.5	1.5	100.0
	Total	390	100.0	100.0	

Table 4.24 Participant responses on the role of transferring patient data outside India

- Table 4.25 illustrates the study of participants 'perspectives on the presence of a distinct provision for the transfer of Electronic Medical Records (EMR) in India. The data exhibits a heterogeneous range of viewpoints among participants. Around 42.6% of participants express either a strong agreement (14.1%) or agreement (28.5%) on the existence of a dedicated provision for the transfer of Electronic Medical Records (EMR) in India. Participants in the study demonstrated a notable level of awareness and recognition regarding the existence of legislation or norms that control the transmission

of electronic medical records. Approximately 47.7% of respondents belong to the 'Neutral' category, suggesting a significant portion of those who are either unsure or do not have a clear stance on the presence of regulations for EMR transfer in India. This indicates a requirement for clarification or heightened understanding among this group regarding the regulatory framework pertaining to EMR transfers. 8.7% of the respondent's express disagreement with the idea of having a special provision for EMR transfer, placing them in the 'Disagree' category. This viewpoint is held by a small number of respondents who may doubt or lack knowledge about the presence of specific legislation in this matter. Merely a negligible proportion, 1.0%, belongs to the 'Strongly Disagree' classification, signifying a profound opposition to the inclusion of a particular provision for EMR transfer in India. This indicates a distinct and limited group of responders who strongly oppose the concept of such laws.

Q25		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	55	14.1	14.1	14.1
	2	111	28.5	28.5	42.6
	3	186	47.7	47.7	90.3
	4	34	8.7	8.7	99.0
	5	4	1.0	1.0	100.0
	Total	390	100.0	100.0	

Table 4.25 Participant response on the rule regulation to transfer of Electronic Medical Record in India

- Table 4.26 discloses data on how respondents perceive the likelihood of patient data or Electronic Medical Record (EMR) breaches in India up until the year 2023. The data exhibits a spectrum of viewpoints among the participants. A total of 26.9% of participants, comprising 9.7% who strongly agree and 17.2% who agree, believe that there have been no instances of patient data or EMR leak in India up until 2023. These findings indicate that only a small portion of the participants have a favorable perspective, demonstrating assurance or trust in the protection of patient data inside the

Indian healthcare system. 49.2% of the respondents belong to the 'Neutral' category, suggesting a significant proportion of those who are either unsure or do not have a clear perspective on the prevalence of data breaches. The absence of a definitive position may arise from insufficient knowledge, limited awareness, or differing degrees of trust in the existing security procedures. 18.2% of respondents disagree, indicating a subgroup who believe that there have been instances of patient data or EMR breaches in India up until 2023. This perspective could be shaped by apprehensions over data security protocols or knowledge of documented occurrences. Only a small proportion, namely 5.6%, falls under the 'Strongly Disagree' category, which suggests that there is a small but distinct group of respondents who firmly deny the notion that there have been no instances of patient data or EMR breaches in India up until 2023.

Q26		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	38	9.7	9.7	9.7
	2	67	17.2	17.2	26.9
	3	192	49.2	49.2	76.2
	4	71	18.2	18.2	94.4
	5	22	5.6	5.6	100.0
	Total	390	100.0	100.0	

Table 4.26 Participants response on the cases of patient sensitive data or EMR breach till 2023

- According to Table 4.27, a substantial majority of participants, up to 78.5%, either strongly agree (30.0%) or agree (48.5%) that Electronic Medical Record (EMR) data is classified as Sensitive Data. There is a general agreement among participants about the sensitive nature of EMR information, emphasizing the significance and confidentiality of patient medical records. Only a small portion of the participants (17.2%) remains neutral, suggesting that there is a group that is unsure or has differing levels of opinion regarding the sensitivity of EMR data. 4.3% of individuals hold a dissenting opinion, indicating a minority stance that may arise from varying

viewpoints on the sensitivity of EMR data. In addition, a small proportion (1.0%) strongly disagrees with the statement.

Q27		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	117	30.0	30.0	30.0
	2	189	48.5	48.5	78.5
	3	67	17.2	17.2	95.6
	4	13	3.3	3.3	99.0
	5	4	1.0	1.0	100.0
	Total	390	100.0	100.0	

Table 4.27 Participants responses on that EMR data is a sensitive data.

- Table 4.28 demonstrates the respondent's viewpoints regarding individual m that the improper use of patient Electronic Medical Records (EMR), such as altering information in the patient's medical record by an individual, negatively impacts the patient's health. Out of all the participants, a significant majority of 97.0% either strongly agree (42.6%) or agree (54.4%) with the given statement. The significant consensus highlights the universal acknowledgment among participants that unauthorized alterations or improper use of patient EMR can have adverse consequences on the patient's well-being. A minority, comprising only 1.8% of the population, holds a dissenting opinion, suggesting that their viewpoint may stem from divergent viewpoints of the potential consequences of misusing EMR on patient well-being. A negligible proportion (1.2%) vehemently opposes the assertion, indicating a minute yet distinct subset of participants who firmly refute the notion that patient EMR misuse can result in detrimental consequences on the patient's well-being.

Q28		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	141	36.2	42.6	42.6
	2	180	46.2	54.4	97.0
	4	6	1.5	1.8	98.8

	5	4	1.0	1.2	100.0
	Total	331	84.9	100.0	
Missing	System	59	15.1		
Total		390	100.0		

Table 4.28 Participants responses on the misuse of patients sensitive data or the EMR records such as altering information that impacts the patient's health.

iv. Internet of Things (IoT) and wearables implementation in Healthcare Sector

- Table 4.29 presents respondents 'viewpoints on the effects of integrating emerging technologies, such as the Internet of Things (IoT) and Artificial Intelligence (AI), in the healthcare industry. The data reveals a substantial consensus among participants, with 81.5% expressing either strong agreement (39.7%) or agreement (41.8%) about the transformative impact of emerging technologies such as IoT and AI on the healthcare industry. Participants widely acknowledge that these technological breakthroughs are causing significant changes in the healthcare industry. Approximately 16.9% of the respondents have a neutral position, indicating a group that may have differing levels of opinion or doubt on the influence of new technologies on the healthcare industry. Only a minute fraction, specifically 1.5%, holds a contrary opinion, suggesting a minority standpoint that could be based on skepticism or divergent viewpoints regarding the revolutionary impacts of IoT and AI in the healthcare sector.

Q29		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	155	39.7	39.7	39.7
	2	163	41.8	41.8	81.5
	3	66	16.9	16.9	98.5
	4	4	1.0	1.0	99.5
	5	2	.5	.5	100.0
	Total	390	100.0	100.0	

Table 4.29 Participants responses on implementing technology like IoT and AI changes the working of healthcare sector

- Table 4.30 depicts the opinions of the participants regarding the assertion that most wearable devices utilized in the healthcare industry, such as fitness trackers, remote patient monitors, chest straps, and temperature sensors, are built upon Internet of Things (IoT) technology. The results indicate a high level of consensus among participants, with 81.8% expressing either strong agreement (32.3%) or agreement (49.5%) about the predominant use of IoT technology in healthcare wearable devices. The extensive consensus indicates the broad acknowledgment that IoT is essential for the performance and connectivity of wearable healthcare equipment. A significant proportion (15.1%) maintain a neutral position, suggesting a group that may have differing levels of opinion or uncertainty regarding the predominance of IoT technology in these products. Only a small fraction, specifically 2.6%, holds a contrary opinion to the statement. This suggests a minority viewpoint that could be based on skepticism or conflicting interpretations of the level of IoT integration in healthcare wearables. A minute fraction (0.5%) vehemently opposes the assumption, denoting a negligible portion of respondents who firmly dispute the notion that most healthcare wearable gadgets depend on IoT technology.

Q30		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	126	32.3	32.3	32.3
	2	193	49.5	49.5	81.8
	3	59	15.1	15.1	96.9
	4	10	2.6	2.6	99.5
	5	2	.5	.5	100.0
	Total	390	100.0	100.0	

Table 4.30 Participants responses on the wearable technology used in healthcare is based on IoT technology.

- The responses to the questions about whether new technologies, namely the application of AI and IoT in the healthcare industry, are subject to rules and regulations in India are summarized in Table 4.31. The data indicates that 65.1% of the respondents either strongly agree (24.4%) or agree (40.8%) with the statement that India does not have sufficient restrictions for the use of IoT and AI in the healthcare industry. Participants in the healthcare arena express a significant degree of anxiety or doubt over the regulatory structure that governs these technologies. Approximately 27.2% of the participants have a neutral position, indicating a group that may have differing levels of opinion or uncertainty regarding the presence of guidelines and regulations for Internet of Things (IoT) and Artificial Intelligence (AI) in the healthcare sector. A small proportion, namely 6.2%, holds a dissenting opinion about the assertion, suggesting that their viewpoint may be based on the belief that there are existing laws governing the use of these technologies in the healthcare industry. A minute fraction (1.5%) vehemently opposes the assertion, comprising a negligible portion of participants who outright deny the notion that there are no guidelines and protocols for the integration of IoT and AI in healthcare in India.

Q31		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	95	24.4	24.4	24.4
	2	159	40.8	40.8	65.1
	3	106	27.2	27.2	92.3
	4	24	6.2	6.2	98.5
	5	6	1.5	1.5	100.0
	Total	390	100.0	100.0	

Table 4.31 Participants responses on the viewpoint of Indian System in regularizing the devices based on technology like IoT, AI in the healthcare sector

- The approaches of the respondents on the possibility that the adoption of new technologies such as the Internet of Things (IoT) and AI-based devices in the

healthcare industry may result in a rise in incidents such patient data breaches, and smart medical device malfunctions are shown in Table 4.32. The results indicate that a substantial majority, accounting for 69.2%, either strongly supports (23.8%) or supports (45.4%) the notion that the introduction of IoT and AI-driven devices in healthcare could lead to an increase in incidents such as patient data breaches and the malfunctioning of intelligent medical devices. Participants in the healthcare sector are showing a significant level of worry and understanding of the potential risks that come with implementing these technologies. Around 24.6% of participants have a neutral position, indicating a group that may have differing levels of opinion or doubt regarding the probability of more breaches and failures. Only a small fraction, namely 5.6%, holds a different opinion, suggesting that their perspective may be based on a strong belief in the safety and dependability of Internet of Things (IoT) and artificial intelligence (AI) equipment in the healthcare sector. A minute fraction (0.5%) vehemently opposes the assertion, comprising a negligible portion of participants who firmly reject the notion that the adoption of novel technologies will result in a rise in occurrences such as patient data breaches and malfunctions of intelligent medical devices.

Q32		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	93	23.8	23.8	23.8
	2	177	45.4	45.4	69.2
	3	96	24.6	24.6	93.8
	4	22	5.6	5.6	99.5
	5	2	.5	.5	100.0
	Total	390	100.0	100.0	

Table 4.32 Participants responses on the adoption of new technology based on IoT, AI in the healthcare sector increase the cases such patient data breaches, and smart medical device malfunctions.

- Table 4.33 shows insights into respondent's perspectives regarding the claim that attackers can exploit patient's sensitive data and put their lives at risk. The data reveals that a substantial majority of participants, amounting to

77.9%, either strongly concurs (29.5%) or concurs (48.5%) with the statement. This indicates that the participants are widely acknowledging the possible dangers linked to the improper use of patient-sensitive data by attackers, which could have severe implications for patient's well-being. Around 17.7% of participants had a neutral position, indicating a group that may have different levels of opinion or uncertainty about the probability and seriousness of these attacks. 3.1% of individuals have a dissenting opinion, maybe due to their faith in the effectiveness of the security measures implemented to safeguard patient data. Only a minute fraction (1.3%) vehemently opposes the assertion, comprising a negligible portion of participants who outright reject the notion that attackers can use patient data to the point of endangering lives.

Q33		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	115	29.5	29.5	29.5
	2	189	48.5	48.5	77.9
	3	69	17.7	17.7	95.6
	4	12	3.1	3.1	98.7
	5	5	1.3	1.3	100.0
	Total	390	100.0	100.0	

Table 4.33 Participants responses on the patient data be misused by the attacker and lead to threaten the patient life.

- The perspectives of the respondents regarding the scope of the Digital Personal Data Protection Act, 2023 in India with respect to sensitive patient data are presented in Table 4.34. The research reveals that a total of 52.3% of participants either strongly agree (13.3%) or agree (39.0%) with the assertion that the Digital Personal Data Protection Act, 2023 lacks protections for patient sensitive data. This indicates a significant level of apprehension or conviction among participants that the current regulation may not sufficiently address the safeguarding of sensitive patient data. Approximately 41.3% of respondents had a neutral posture, suggesting that they may have differing

opinions or uncertainties about the coverage of patient sensitive data in the Digital Personal Data Protection Act. A small proportion, namely 4.6%, hold a dissenting opinion, indicating a perspective that may be based on a strong belief in the effectiveness of the legal measures in safeguarding patient confidential information. Only a minute fraction (1.8%) vehemently opposes the statement, comprising a negligible portion of participants who firmly assert that the Digital Personal Data Protection Act, 2023 sufficiently encompasses provisions pertaining to sensitive patient data.

Q34		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	52	13.3	13.3	13.3
	2	152	39.0	39.0	52.3
	3	161	41.3	41.3	93.6
	4	18	4.6	4.6	98.2
	5	7	1.8	1.8	100.0
	Total	390	100.0	100.0	

Table 4.34 Participants responses on India's Digital Personal Data Protection Act, 2023 is not cover the provisions related to patient sensitive data.

- Table 4.35 shows the viewpoints of the participants on the assertion that Europe and the US are more capable than India in addressing concerns related to safeguarding patient-sensitive data. The results indicate that a substantial majority, accounting for 69.0% of participants, either strongly concurs (24.6%) or concurs (44.4%) with the statement. The participant's viewpoint implies that Europe and the US are perceived to have a superior and more efficient system for addressing concerns regarding the safeguarding of patient-sensitive information, in contrast to India. Around 28.5% of participants hold a neutral viewpoint, suggesting a group that may have differing levels of opinion or doubt about the respective capabilities of these locations in safeguarding patient data. A small fraction, namely 0.8%, holds a differing opinion, implying a perspective that could be based on trust in India's ability to properly address concerns over the safeguarding of patient-

sensitive data. Only a negligible fraction (1.8%) vehemently opposes the assertion, comprising a small portion of participants who firmly hold the belief that India is better equipped than Europe and the US in safeguarding patient-sensitive data.

Q35		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	96	24.6	24.6	24.6
	2	173	44.4	44.4	69.0
	3	111	28.5	28.5	97.4
	4	3	.8	.8	98.2
	5	7	1.8	1.8	100.0
	Total	390	100.0	100.0	

Table 4.35 Participants responses on Europe and United States is in better position than India to regularize the patient sensitive data.

- The opinions of respondents on the claim that the US has rules pertaining to the security of data stored by Internet of Things (IoT) devices are shown in Table 4.36. The data reveals that a substantial majority, accounting for 61.0% of participants, either strongly concurs (17.2%) or concurs (43.8%) with the statement. Participants in the study hold the belief that the United States has implemented legal structures to address the security of data stored by IoT devices. Approximately 35.6% of respondents hold a neutral position, suggesting a group that may have differing levels of opinion or doubt regarding the presence and effectiveness of regulations concerning IoT device data security in the United States. A small fraction, namely 2.3%, holds a differing opinion, indicating a perspective that may be based on skepticism over the existence or effectiveness of legislation pertaining to the security of IoT device data in the United States. A minute fraction (1.0%) vehemently opposes the statement, comprising a negligible portion of participants who outright dispute the notion that the US has legislation pertaining to the safeguarding of data stored by IoT devices.

Q36	Frequency	Percent	Valid Percent	Cumulative Percent

Valid	1	67	17.2	17.2	17.2
	2	171	43.8	43.8	61.0
	3	139	35.6	35.6	96.7
	4	9	2.3	2.3	99.0
	5	4	1.0	1.0	100.0
	Total	390	100.0	100.0	

Table 4.36 Participants responses on US have laws related to regularization of IoT devices

- Regarding the claim that Europe has sufficient laws to safeguard patient-sensitive data, Table 4.37 shows the responses of the respondents. The data indicates that a total of 57.4% of the participants either strongly agree (17.7%) or agree (39.7%) with the statement. This suggests that most respondents believe that Europe has implemented sufficient laws to protect patient-sensitive data. Around 38.7% of the participants hold a neutral position, suggesting that they may have different levels of opinion or uncertainty about the effectiveness of European legislation in safeguarding patient-sensitive data. A small proportion, namely 2.8%, holds a differing opinion, indicating a perspective that may be based on doubt on the sufficiency of current legislation in Europe. Only a minute fraction (1.0%) vehemently opposes the assertion, comprising a negligible portion of participants who outright reject the notion that Europe possesses adequate regulations to safeguard patient-sensitive data.

Q37		**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	1	69	17.7	17.7	17.7
	2	155	39.7	39.7	57.4
	3	151	38.7	38.7	96.2
	4	11	2.8	2.8	99.0
	5	4	1.0	1.0	100.0
	Total	390	100.0	100.0	

Table 4.37 Participants response on that Europe has sufficient laws to safeguard patient-sensitive data.

- Table 4.38 illustrates the viewpoints of the respondents regarding the proposition that India should adopt or modify its laws concerning the safeguarding of patient-sensitive data by examining the legal structures of the European Union (EU) and the United States. The results indicate that a substantial majority, accounting for 68.7% of participants, either strongly concurs (25.6%) or concurs (43.1%) with the statement. There is a widespread belief among participants that India should carefully examine and maybe modify its laws by taking inspiration from the legal systems of the European Union and the United States to safeguard patient-sensitive data. Around 27.2% of participants hold a neutral position, suggesting a group that may have differing levels of opinion or doubt on the necessity for India to harmonize its legal systems with those of the European Union and the United States. 3.1% of individuals have a dissenting opinion, maybe due to their confidence in the current legislative measures in India that safeguard patient-sensitive data. Only a minute fraction (1.0%) vehemently opposes the notion, comprising a negligible portion of participants who out rightly reject the proposition of India adopting or modifying its legislation in accordance with the legal systems of the European Union and the United States.

Q38		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	100	25.6	25.6	25.6
	2	168	43.1	43.1	68.7
	3	106	27.2	27.2	95.9
	4	12	3.1	3.1	99.0
	5	4	1.0	1.0	100.0
	Total	390	100.0	100.0	

Table 4.38 Participants responses on India should adopt or modify its laws concerning the safeguarding of patient-sensitive data by examining the legal structures of the European Union (EU) and the United States

4.4.7. Result of Survey

To summarize, the thorough examination of the survey data offers a detailed comprehension of respondent opinion on several facets of healthcare, patient confidentiality, and the implementation of developing technologies in India. The study, based on 390 responses from a varied sample of 400 individuals, provides useful insights into the demographic distribution, stakeholder representation, and age dynamics among the participants.

The gender distribution demonstrates a near parity, with females comprising 49% of the population, males comprising 50.5%, and 0.5% remaining undeclared. The presence of an equal number of males and females in this study contributes to its comprehensiveness, allowing for a more thorough examination of viewpoints from both genders.

The stakeholder engagement is characterized by a broad composition, consisting of 5.1% doctors, 10.5% advocates, 25.9% legal scholars, and 58.5% individuals from various other backgrounds. This inclusive representation guarantees a thorough examination of viewpoints, with a particular focus on legal experts and the perspectives of other stakeholders.

The examination of age distribution reveals a significant prevalence of individuals between the ages of 19 and 25, comprising 55.4% of the responses. By focusing on this specific demography, we can gain significant insights into the opinions of the younger age group on the themes being investigated. This contributes to a more thorough understanding of the perspectives that vary throughout different generations.

Participant's perspectives on legislation pertaining to privacy, as well as privacy within the family, relationships, marriage, and personal space, indicate a widespread agreement on the significance of privacy in these areas. Consensus exists that privacy is important in these circumstances, providing a thorough comprehension of cultural attitudes towards privacy issues.

The paper-based medical record system is a cause for concern, as a significant number of people (89.2%) recognize the possibility of losing records and believe that technological advancements are necessary in the healthcare system (90.8%). Furthermore, the participant's express high endorsement for the use of Electronic Medical Record (EMR) systems in India, with 84.9% of them underlining the perceived advantages of migrating from traditional paper-based records.

The examination of participant's viewpoints on many facets of EMR, such as the necessity of EMR, cloud-based storage of patient data, and perceptions of EMR system security, reveals a favorable predisposition towards technological progress

in the healthcare field. Nevertheless, there exists a wide range of perspectives about matters such as unauthorized access to patient data, the implementation of Internet of Things (IoT) and Artificial Intelligence (AI), and the effectiveness of legislative measures. These divergent viewpoints highlight the intricate nature of beliefs held by the participants.

Concisely, the study offers an extensive and meticulous examination of participant's viewpoints on vital elements of healthcare, patient confidentiality, and the acceptance of technology in India. The results emphasize the necessity for ongoing investigation, public consciousness, and policy deliberations to tackle the complex obstacles and possibilities in the changing field of healthcare information management.

4.5. Conclusion

The healthcare system in India exhibits a dual structure, encompassing both public and private healthcare providers. Government-managed public healthcare endeavors to address the healthcare requirements of the general populace, with a specific focus on underserved rural regions. Nevertheless, persistent issues in the healthcare sector include insufficient infrastructure, a scarcity of healthcare experts, and geographical inequities. Despite the notable advancements made, the healthcare system continues to encounter persistent obstacles, one of which is the division between urban and rural areas in terms of healthcare accessibility and quality. Prominent trends in the realm of technology include the widespread use of Electronic Health Records, the utilization of telemedicine, the integration of Artificial Intelligence, and the proliferation of the Internet of Things. The COVID-19 pandemic has highlighted the imperative for a resilient healthcare infrastructure, prompting initiatives to enhance capacity and implement vaccination campaigns. India continues to be a key hub for medical tourism, mostly attributed to the high standard of healthcare services offered at relatively affordable prices.

The advancements that have been made in the field of healthcare yields significant advantages, although it also introduces a variety of obstacles. One notable obstacle pertains to the ethical and legal implications associated with nascent technologies, such as genetic manipulation and artificial intelligence in the realm of medical diagnosis and therapy. The complexity around patient

privacy, patient data storage, inter-state movement of patient data, and data security is heightened in the current era of networked health systems and electronic health records. To effectively tackle these difficulties, it is imperative to foster a collective endeavor involving healthcare professionals, politicians, and technology developers. This collaborative approach is crucial to ensure that breakthroughs in healthcare lead to enhanced patient outcomes, while simultaneously avoiding the exacerbation of pre-existing healthcare inequities. The current legislation in India pertaining to the protection of patient data, regulations for Electronic Medical Record Systems, and the smart medical device system is insufficient in safeguarding and ensuring the security of patient data. There exists a necessity for a comprehensive set of laws that governs the emerging field of medical devices, as well as regulations pertaining to the safeguarding of patient's data. Further an empirical survey has been conducted among various stakeholders, regarding their knowledge and awareness about their own sensitive data. After analysis of the responses, it could be said that the consensus among participants in a study on privacy legislation and healthcare technology in India is that privacy is highly significant in the domains of family, relationships, and personal space. Worries regarding the susceptibility of paper-based medical records lead 89.2% of individuals to endorse technology progress, with 90.8% expressing support for Electronic Medical Record (EMR) systems. Although there is generally a favorable view of the advantages of EMR (Electronic Medical Records), there are differing viewpoints about concerns such as data security, unauthorized access, and the involvement of IoT (Internet of Things) and AI (Artificial Intelligence). This study emphasizes the importance of continuous research, public knowledge, and policy deliberations to navigate the changing field of healthcare information management in India.

During the period of technological advancement, healthcare has witnessed the integration of sophisticated medical gadgets. To achieve a harmonious integration of law and technology, it is imperative to undertake the task of reforming or amending existing legal frameworks. The European Union (EU) and the United States (US) are two nations that, in response to the rapid advancement of technology, have been introducing and implementing new

laws and policies aimed at striking a balance in protecting the interests of patients. There exist legal frameworks that govern the utilization of cutting-edge medical equipment incorporating technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI). Moreover, the categorization of patient data and the designated processing methodologies exhibit distinct variations. The subsequent chapter provides a comprehensive summary of legislation in the European Union (EU) and the United States (US), while also offering a comparative analysis of Indian laws.

CHAPTER 5

A COMPARATIVE ANALYSIS OF EXISTING LAW AND LEGISLATION RELATED TO ELECTRONIC MEDICAL RECORD AND UPGRADED MEDICAL DEVICES IN EUROPEAN UNION, UNITED STATES WITH INDIA

5.1. Introduction

Big data is all about the strategic and channelized use of data for the purposes foreign to the purpose for which they were collected(Berberich & Steiner, 2016). Everything from us invokes the use of "big data" technologies in medicine. "Big data" is generally understood to mean analyzing particularly large volumes, variety, and velocity of data(I. Lee, 2017), and often includes information that was originally collected for different purposes. "Everything from us" implies the increasing collection of health data during medical progress: resident doctors, hospitals, and health insurance companies keep patient files in electronic form; advanced devices used in healthcare; digital health apps accompany us in real-time every step of the way(*Harnessing the Power of Data in Health*, 2017). More and more new medical devices in hospitals and in laboratories, which previously offered independent and stand-alone functionalities, are now integrated into networks and deliver large amounts of data to be further processed and stored via clinic information systems ("CIS") and software(*What Is a Clinical Information System (CIS)?*, 2021).

Medication and treatment options tailored to the patient's specific life circumstances, environmental factors, and biological-genetic predisposition are developed under the terms "precision medicine"(Collins & Varmus, 2015) and "pharmacogenetics," i.e., medication tailored to the genetic conditions of the patient(Scott, 2011).

The collection of health data offers opportunities for better analysis of disease factors, improved diagnostic methods, and higher chances of finding cures as well as a reduction of medical costs and an increased efficiency of the healthcare system(Manyika et al., 2011). At the same time, patients, physicians, researchers, and developers face new risks as a result of the processing of the collected data(Viceconti et al., 2015).These risks range from discrimination and stigmatization based on the data obtained to unwanted knowledge about one's own health and even the fraudulent misuse of data or blackmailing(Seh et al., 2020).

The protection of one's privacy and data are a global issue. Many international treaties and national constitutions refer, expressly or impliedly, to privacy as a core principle or objective(Determann, 2019). On the national level, the regulations differ from each other, especially when it comes to health data. In Europe, the processing of health data is regulated by general, omnibus data processing regulations. In most countries, in addition to data privacy and data protection laws, physicians must protect patient confidentiality under laws or regulations concerning professional responsibilities.

This chapter analyzes the data protection rules, regulations, and legislation of the European Union (EU) and the United States (US) as they pertain to the novel problems brought about by the development of the healthcare industry. The scenario in which patient data is compromised, and the responses of these nations. Can patient information be kept safe under the new Medical Device Regulation system?

5.2. United States and Europe

5.2.1. Healthcare system in US

Accounting for one-third of global sales, the US is the largest pharmaceutical market and is expected to continue to grow at an average annual rate of over 6% per year(Keehan et al., 2020). It is also the third most populous country in the world, with a population of over 336,035,021 people(*Population Clock*, n.d.). The global healthcare market will reach $665.37 billion by 2028, according to Verified Market Research. US national healthcare expenditure reached $4.1 trillion in 2020, or $12,530 per person, and is estimated to reach

$6.2 trillion by 2028, per the Centers for Medicare and Medicaid Services(*US Healthcare Industry in 2023: Analysis of the Health Sector, Healthcare Trends, & Future of Digital Health*, 2023). The healthcare system is one of the most complex among industrialized countries, described as a hybrid system, in which healthcare facilities are provided by the public sector (the federal government, state, and local governments), the private sector (private insurers and businesses), and the consumers (out-of-pocket expenses and self-pay). Traditionally much slower than other industries at adopting digital technologies, healthcare incumbents were finally pushed to digitize everyday systems amid the coronavirus pandemic. The crisis catalyzed a virtual care boom that's continuing to change the fabric of the entire US healthcare ecosystem(*US Healthcare Industry* , 2022). The digital health industry has been able to react quickly with the help of investors, who've been shoveling cash their way: In the first three quarters of 2020 alone, US digital health startups raked in more cash than ever before. Some of the most widely adopted healthcare trends include Electronic Health Records (EHRs), Social Determinants of Health (SDOH), Wearables and Healthcare interoperability.

5.2.2. Healthcare system in EU

The healthcare system inside the European Union (EU) exhibits a wide array of structures and practices because each member state upholds its own distinct national healthcare system. Nevertheless, the European Union (EU) endeavors to promote specific shared values and standards to guarantee a minimum degree of quality and accessibility in healthcare. The European Union places significant emphasis on the significance of comprehensive healthcare coverage, with the objective of ensuring that all individuals have equitable access to fundamental medical services. The healthcare systems of member states commonly integrate both public and private components, wherein government-funded services coexist alongside private healthcare providers. The European Union (EU) additionally fosters collaboration among its member states to effectively tackle shared health issues, advance research, and development endeavors, and guarantee the seamless movement of patients across national borders. Although there are differences in the structure and funding of healthcare systems among European Union (EU) member

states, the primary objective remains the provision of accessible and cost-effective healthcare services of superior quality to all individuals within these nations.

The European Union (EU) has made notable advancements in the field of healthcare technology, with a primary emphasis on enhancing patient outcomes, efficiency, and accessibility. The incorporation of digital technologies has had a significant impact, since electronic health records have become increasingly common, improving the organization of healthcare services, and enabling the seamless sharing of information among healthcare professionals. The utilization of telemedicine has become increasingly prominent in recent years, facilitating the provision of remote consultations, monitoring, and the delivery of select healthcare services. This advancement has played a significant role in enhancing accessibility to healthcare, particularly in regions that are geographically isolated or lack adequate medical resources. Furthermore, there has been a notable increase in the utilization of health applications, wearable technologies, and remote patient monitoring instruments, enabling individuals to actively engage in the management of their healthcare. The utilization of artificial intelligence (AI) and machine learning applications is becoming more prevalent in the healthcare field. These technologies are being used for diagnostic reasons, optimizing treatment plans, and providing predictive analytics. As a result, healthcare practitioners are gaining significant insights from these applications. The European Union (EU) has demonstrated a proactive approach in promoting collaboration and standardization within the field of health technology development. This initiative aims to guarantee interoperability and data security among member states. Consequently, the ongoing progress in healthcare technology is significantly altering the healthcare sector, facilitating the provision of healthcare services that are tailored to individual needs, more streamlined, and readily available to the various populace inside the European Union.

5.3. Different Rules and Regulations pertaining to Patient Sensitive Data and the Medical Devices in United States and Europe

Within the European Union (EU), the governance of patient data and medical devices is subject to separate regulatory regimes. The General Data Protection policy (GDPR) is an extensive privacy policy that aims to protect the processing of patient data, encompassing electronic medical record, with a particular focus on promoting openness, obtaining consent, and ensuring data security. Concurrently, the Medical Devices Regulation (MDR) imposes high criteria for the safety and performance of medical devices, mandating thorough assessments, clinical evaluations, and post-market surveillance to assure continuing compliance. Patient data protection in the United States is primarily overseen by the Health Insurance Portability and Accountability Act (HIPAA), which imposes requirements for the secure management of personally identifiable health information. The regulatory authority responsible for the oversight of medical devices is the Food and Drug Administration (FDA). To ensure the effectiveness and safety of these products, the FDA employs a combination of pre-market approval, post-market surveillance, and quality system standards. Both the EU and the US consistently modify their regulatory frameworks in response to technology improvements, prioritizing the preservation of patient safety, data integrity, and the ethical utilization of health information. It is crucial for businesses operating in the healthcare sector to adhere to these standards to safely traverse the intricate landscape of patient data and medical device management. The overall structure of the legislation relating to patient data protection and medical devices will be shown in Figure 5.1.

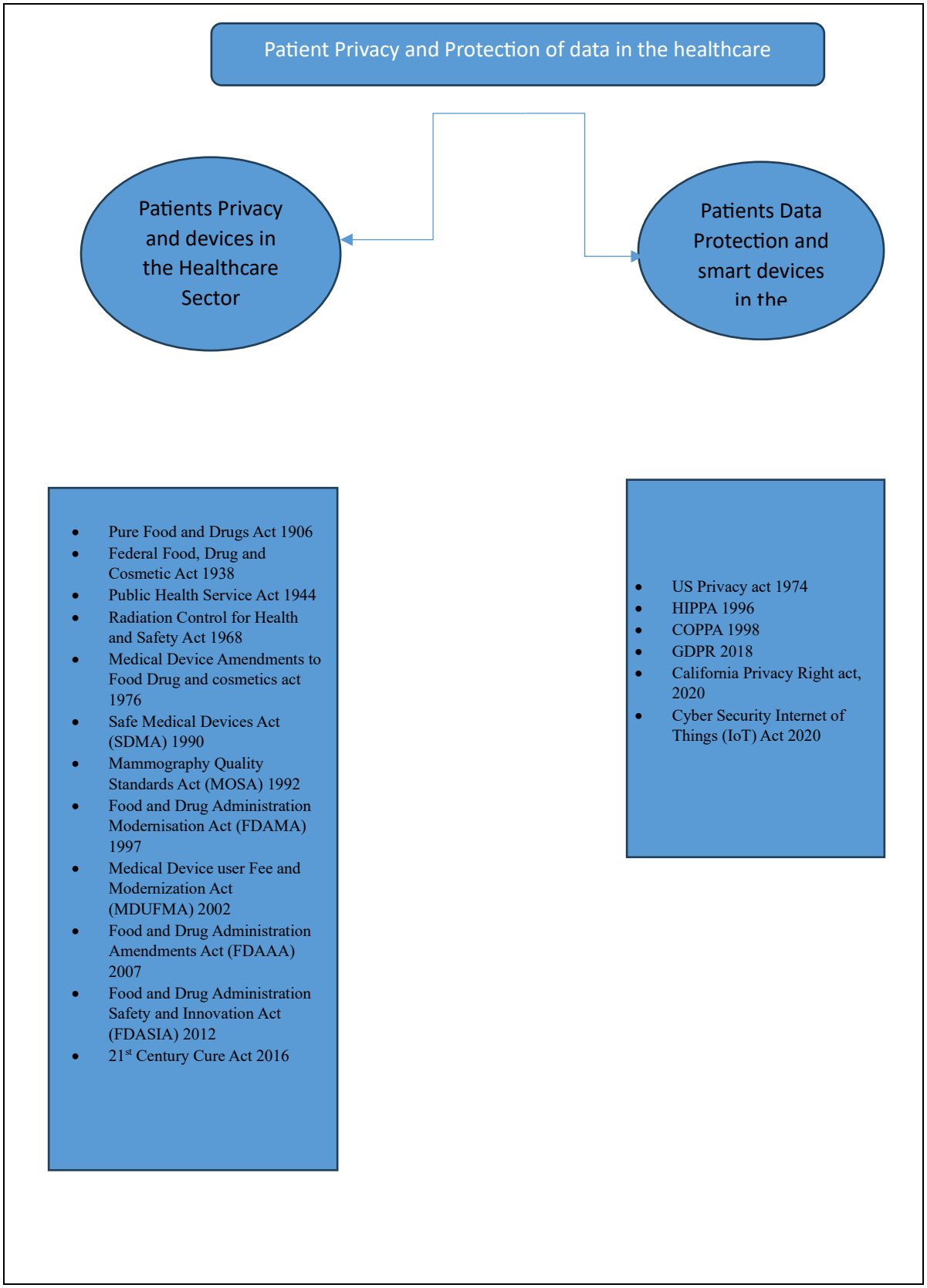

Figure 5.1 Classification of Rules, Regulations and Laws related to Electronic Medical Records and the patient data.

5.3.1. Rules, Regulation, and the laws specifically to Patient Privacy Rights and medical devices regulation in the Healthcare

The regulation of patient privacy and medical devices is overseen by the European Union (EU) and the United States (US) through a series of legislative acts. These acts include *the Pure Food and Drugs Act of 1906, the Federal Food, Drug and Cosmetic Act of 1938, the Public Health Service Act of 1944, the Radiation Control for Health and Safety Act of 1968, the Medical Device Amendments to the Food, Drug, and Cosmetics Act of 1976, the Safe Medical Devices Act (SDMA) of 1990, the Mammography Quality Standards Act (MOSA) of 1992, the Food and Drug Administration Modernization Act (FDAMA) of 1997, the Medical Device User Fee and Modernization Act (MDUFMA) of 2002, the Food and Drug Administration Amendments Act (FDAAA) of 2007, the Food and Drug Administration Safety and Innovation Act (FDASIA) of 2012, and the 21st Century Cure Act of 2016*.

A. Pure Food and Drugs Act 1906

The Pure Food and Drug Act of 1906 holds significant importance as a crucial legislative measure inside the United States, with the primary objective of safeguarding consumers against deceitful tactics pertaining to the manufacturing and labeling of food and pharmaceutical products.

During the late 19th and early 20th centuries, a significant number of American consumers were subjected to the use of food and medicinal products that were tainted, falsely labeled, or have other detrimental qualities. The absence of government laws pertaining to the production and labeling of food and drugs further aggravated the problem.

This legislation initiated a notable level of government regulation over the food and drug sectors, thereby guaranteeing that consumers were provided with items that were both safe and accurately labeled. The provisions of the Act were subsequently enlarged and reinforced via the enactment of the Food, Drug, and Cosmetic Act of 1938.

B. The Food, Drug and Cosmetic Act 1938

The Food, Drug, and Cosmetic Act (FDCA) enacted in 1938 is a seminal legislative measure that established the fundamental structure for the contemporary oversight of food products, pharmaceuticals, beauty products, and medical apparatus within the United States. The Act substantially augmented the regulatory authorities vested in the Food and Drug Administration (FDA) and was enacted in reaction to a range of public health calamities and increased apprehensions over the safety of products.

The enactment of the Food, Drug, and Cosmetic Act (FDCA) was partly inspired by the tragic incident known as the "Elixir Sulfanilamide" disaster in 1937. This event involved the distribution of a hazardous formulation of a novel pharmaceutical product, resulting in the loss of more than 100 lives. The incident served as a poignant reminder of the pressing necessity for more stringent rules pertaining to drug safety.

The Food, Drug, and Cosmetic Act (FDCA) enacted in 1938 built upon and superseded the Pure Food and Drug Act of 1906, thereby extending the scope of items subject to regulatory supervision and substantially enhancing the regulatory powers vested in the Food and Drug Administration (FDA). The legislation established the foundation upon which numerous future changes and laws were built, thereby influencing the regulatory framework pertaining to various commodities such as food, pharmaceuticals, and other products. The main provisions that added are:

- The manufacturer was demonstrating the safety of new drug and need of pre-market approval.
- There are provisions that restrict and imposed penalties against the adulteration or misbranding of foods, drugs, cosmetics, and medical devices.
- The manufacturer required that safe tolerances be set for unavoidable poisonous substances in food.
- The FDCA introduced cosmetics and therapeutic devices under federal regulatory authority for the first time.

- The Food and Drug Administration (FDA) has been bestowed with the power to promulgate emergency regulations for specific items in cases when it is imperative to avert an immediate threat to the well-being of the general population.
- The FDA was granted expanded authority to conduct inspections of factories and production facilities to verify their adherence to the Act.

C. The Public Health Service Act 1944

The Public Health Service Act of 1944 (PHSA) was a significant piece of legislation in the United States that played a pivotal role in centralizing and restructuring the country's public health services. The Public Health Service (PHS) was officially founded as a significant Section within the Department of Health, Education, and Welfare (now recognized as the Department of Health and Human Services) with the enactment of the Act. The Public Health Service Act (PHSA) established the position of the Surgeon General as the principal authority within the Public Health Service (PHS), so solidifying their leadership role. This legislation played a crucial part in facilitating the establishment of the National Institutes of Health (NIH), which has since become a prominent organization dedicated to advancing biomedical research. The legislation additionally conferred authority to the Public Health Service (PHS) to oversee and control the manufacturing and distribution of biologics, thereby guaranteeing their safety and effectiveness.

The Act has undergone several amendments to effectively respond to developing public health concerns. These amendments have included the development of specialized health agencies to address specific health issues, as well as the incorporation of measures to tackle modern challenges including bioterrorism and emerging infectious illnesses, hence playing a pivotal role in establishing the public health framework of the United States.

D. Radiation Control for Health and Safety Act 1968

The enactment of the Radiation Control for Health and Safety Act of 1968 was a direct response to apprehensions regarding the possible risks associated

with radiation emissions originating from electronic devices, with a specific focus on X-ray machines.

The main objective of this legislation was to safeguard the general population from the potential risks associated with radiation emitted by electronic items. This was particularly crucial due to the growing prevalence of electronic devices across diverse fields such as healthcare, business, and scientific investigation.

Electronic product manufacturers were obligated to provide certification affirming that their products adhered to the prescribed requirements. In addition, they were required to document any inadvertent radiation incidents and instances of product faults.

The Radiation Control for Health and Safety Act of 1968 revised the Public Health Service Act, granting the Food and Drug Administration (FDA) the jurisdiction to oversee the regulation of electronic items that emit radiation.

The regulation served as a recognition of the potential risks associated with radiation emissions during a period characterized by the swift growth of technology. Over the course of its existence, the Act has undergone multiple revisions in response to advancements in technology and a deeper comprehension of radiation, with the aim of consistently safeguarding public safety.

E. Medical Device Amendments to Food Drug and cosmetics Act 1976

The regulatory jurisdiction of the U.S. Food and Drug Administration (FDA) pertaining to medical devices was substantially augmented by the Medical Device Amendments of 1976. These amendments were enacted to address apprehensions regarding the safety and efficacy of medical devices and were incorporated into the existing Federal Food, Drug, and Cosmetic Act (FD&C Act).

The principal objective was to ascertain the safety and efficacy of medical devices prior to their distribution to customers. Previously, the regulation of medical devices was somewhat less stringent in comparison to that of pharmaceutical medications.

Classification System: The modifications implemented a tri categorization framework for medical devices, predicated on their level of risk:

- Class I medical devices are categorized as low risk, such as bandages. These gadgets are subject to regulatory measures.
- Class II devices, such as powered wheelchairs, are categorized as having a moderate level of danger. These devices are subject to specific regulatory measures in addition to broader regulatory measures.
- Class III medical devices are considered to have a high risk associated with their use. Examples of such devices include pacemakers. To guarantee the safety and efficacy of these gadgets, they necessitate pre-market approval.

The implementation of the Medical Device Amendments of 1976 was prompted by a series of notable medical device failures, which underscored the necessity for enhanced regulatory supervision. The revisions have established a comprehensive regulatory framework for medical devices in the United States, which ensures that these products undergo a rigorous examination process to determine their safety and effectiveness prior to being made available in the market.

F. Safe Medical Devices Act (SDMA) 1990

The Safe Medical Devices Act (SMDA) enacted in 1990 represents a notable legislative measure that bolstered the regulatory infrastructure pertaining to medical devices inside the United States.

The focus of this act was regarding injuries and fatalities associated with devices, the SMDA placed significant emphasis on post-market surveillance. This entailed imposing a requirement on producers of high-risk devices to actively monitor and promptly report any adverse events that occur. One noteworthy aspect is the implementation of the Medical Device Reporting (MDR) system, which required manufacturers as well as user facilities, such as hospitals, to report designated device-related concerns.

Hospitals, nursing homes, and other user facilities were required by regulatory mandates to submit reports on deaths associated with medical devices to both the Food and Drug Administration (FDA) and the respective device maker.

Similarly, reports on serious injuries resulting from device usage were to be exclusively submitted to the manufacturer.

The Safe Medical Devices Act of 1990 held great significance since it comprehensively covered the entire lifespan of medical devices, encompassing their pre-market development and approval processes, as well as their post-market performance evaluation and potential recall procedures. The primary objective of the Safe Medical Devices Act (SMDA) was to strengthen the regulatory capabilities of the Food and Drug Administration (FDA) to mitigate the occurrence of injuries and fatalities associated with medical devices. This legislation sought to provide a more rigorous framework for guaranteeing patient safety and upholding a higher standard of quality in the healthcare industry.

G. Mammography Quality Standards Act (MOSA) 1992

The Mammography Quality Standards Act (MQSA) was enacted in 1992 with the aim of establishing uniformity and enhancing the caliber of mammography services throughout the United States. Its primary objective is to guarantee the dependability and precision of mammograms in the detection of breast cancer. The legislation required that all mammography facilities obtain certification from either the FDA or an authorized certifying entity, as evidence of their compliance with rigorous quality standards.

It was necessary for facilities to retain mammography findings and associated records for a specified period, to provide access to previous mammograms for comparative purposes by patients and their healthcare providers.

The Food and Drug Administration (FDA) has been granted the jurisdiction to enforce the regulations established by the Mammography Quality requirements Act (MQSA), which encompasses the ability to impose penalties, mandate corrective measures, or withdraw certification from facilities that fail to comply with the established requirements.

The Mammography Quality Standards Act of 1992 recognized the significant significance of timely and precise identification of breast cancer. The primary objective of the MQSA was to save a significant number of women by augmenting the dependability and efficacy of mammography as a diagnostic

instrument through the implementation of stringent criteria and the maintenance of continuous adherence.

H. Food and Drug Administration Modernization Act (FDAMA) 1997

The Food and Drug Administration Modernization Act (FDAMA) of 1997 was a significant piece of legislation that sought to restructure and enhance the regulatory procedures of the Food and Drug Administration (FDA). With a primary focus on improving efficiency, FDAMA implemented a "fast track" review mechanism to expedite the approval process for pharmaceuticals targeting severe medical conditions. Additionally, it introduced incentives for drug manufacturers to conduct research on the effects of their products on pediatric populations, offering extended market exclusivity as a reward.

This act advocated for the use of electronic regulatory submissions, thereby establishing a structure for the FDA to accept electronic data submissions. This initiative represented a significant milestone in the agency's efforts to modernize its operational procedures.

The Food and Drug Administration Modernization Act (FDAMA) of 1997 is a significant landmark in the regulatory history of the United States. It signifies the notable progress made in the biomedical industry and the imperative need for a regulatory agency that is more responsive and streamlined. The Act acknowledged the significance of expediting the delivery of crucial treatments to patients, while also prioritizing the safety, effectiveness, and truthful portrayal of therapeutic items.

I. Medical Device User Fee and Modernization Act (MDUFMA) 2002

The enactment of the Medical Device User Fee and Modernization Act (MDUFMA) in 2002 marked a substantial transformation in the regulatory approach of the U.S. Food and Drug Administration (FDA) towards medical devices. The primary objective of this act was to optimize the operational efficiency and efficacy of the Food and Drug Administration's (FDA) procedures pertaining to medical devices, while concurrently guaranteeing their safety and performance. Also, it speeds up reviewing medical devices,

enhances patient accessibility to cutting-edge medical innovations, and upholds stringent criteria for device safety and efficacy.

The user fee refers to the monetary charge imposed on manufacturers who submit pre-market applications, pre-market notifications, and other device-related submissions. The allocation of these monies was designated for the purpose of assisting the FDA in augmenting its personnel and resources, with the objective of speeding up reviewing devices.

This Act placed significant emphasis on the prioritization of aligning regulatory requirements with international standards, with the aim of fostering consistency and facilitating the global sale of products.

The Medical Device User Fee and Modernization Act (MDUFMA) of 2002 demonstrated a dedication to ensuring patient safety while also addressing the requirements of the medical device industry. The Act aimed to enhance and optimize the FDA's approach to medical device regulation through the implementation of a user fee scheme.

J. Food and Drug Administration Amendments Act (FDAAA) 2007

The Food and Drug Administration Amendments Act (FDAAA) of 2007 dramatically increased the jurisdiction and responsibilities of the U.S. Food and Drug Administration (FDA). The primary objective of this act is to enhance the efficacy of safety processes, hence facilitating improved post-market surveillance of pharmaceutical products. This legislation empowers the FDA with the authority to require Risk Evaluation and Mitigation Strategies (REMS) for specific pharmaceuticals, so ensuring that manufacturers effectively address identified or anticipated concerns. There is also mandatory to disclose the results for the clinical trials on ClinicalTrials.gov, ensuring greater transparency in the medical research arena. In addition, the legislation placed more emphasis on the importance of drug safety, implemented stronger methods for ensuring food safety, provided incentives for the development of novel antibiotics, and sought to mitigate conflicts of interest within the advisory committees of the FDA. The FDAAA can be considered a significant legislative achievement, as it effectively

streamlined the operations of the FDA, placing a strong emphasis on patient safety and promoting transparency within the industry.

K. Food and Drug Administration Safety and Innovation Act (FDASIA) 2012

The main objective of the Food and Drug Administration Safety and Innovation Act (FDASIA) was to streamline the licensing procedure for novel pharmaceuticals and medical devices, hence facilitating prompt availability of efficacious therapies to patients. This legislation implemented provisions aimed at bolstering the safety and integrity of the pharmaceutical supply chain.

L. 21st Century Cure Act 2016

The 21st Century Cures Act, which was implemented in December 2016, is a significant healthcare legislation that aims to speed up medical product development and facilitate the timely introduction of novel advancements to patients. The legislation facilitates the modernization of clinical trials by advocating for the incorporation of real-world evidence and patient experience data. The Cures Act implements strategies aimed at improving the interoperability of electronic health records (EHRs), hence facilitating efficient communication across different systems. Additionally, it places significant emphasis on granting patients the ability to access their personal health data. Furthermore, the legislation enhances the financial resources allocated to the Food and Drug Administration (FDA), streamlines its recruitment procedures, and advances initiatives pertaining to mental health, suicide prevention, and the availability of orphan drugs. The 21st Century Cures Act is a comprehensive endeavor aimed at modernizing and optimizing healthcare systems, with a particular focus on patient-centricity and expeditious innovation.

5.3.2. Rules, Regulation, and the laws pertaining to Patient Data Protection and the upgraded medical devices in the Healthcare

The United States and the European Union have implemented a range of legislative measures, regulations, and recommendations to standardize the Electronic Medical Record system. Additionally, they have established protocols for the regulation of innovative medical equipment that utilize emerging technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI). Nevertheless, it is important to note that these laws exhibit a high degree of specificity in terms of their focus and subject matter, thereby encompassing a relatively narrow range of issues. The present study does not provide an exhaustive examination of the comprehensive legislation pertaining to privacy and data protection within the healthcare industry in the United States at both the federal and state levels, as well as in European countries. The subsequent part will endeavor to elucidate the fundamental theme of the legislation, which is:

i. United States Privacy Act of 1974

ii. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a federal law in the United States that establishes regulations for the protection of individual's health information.

iii. The Children's Online Privacy Protection Act (COPPA) of 1998 is a federal law in the United States that aims to safeguard the privacy of children under the age of 13 by regulating the collection and use of their personal information online.

iv. The General Data Protection Regulation (GDPR) of 2018 is a European Union regulation that governs the protection and privacy of personal data of individuals inside the EU and the European Economic Area

v. The California Privacy Rights Act of 2020 and the Cyber Security Internet of Things (IoT) Act of 2020 are legislative acts in California that address privacy and cybersecurity concerns. The former enhances privacy rights and consumer protections, while the latter focuses on securing internet-connected devices.

A. The Privacy Act, 1974

The Privacy Act of 1974, officially known as Public Law No. 93-579 and recorded as 88 Stat 1896 on December 31, 1974, was enacted as 5 U.S.C. § 552a in 2018. It assumed its role as the primary legislation regulating the management of personal data inside the federal government on September 27, 1975. This legislation represents the initial legal framework addressing the safeguarding of personal information. The Privacy Act was implemented following the Watergate and Counterintelligence Program (COINTELPRO) scandals, which entailed unauthorized surveillance on opposition political parties and individuals labeled as "subversive." Its purpose was to rebuild public confidence in the government and to confront what was perceived as a significant danger to American democracy during that period.

The Department of Health, Education and Welfare (HEW) presented a report in 1973 that examined the potential privacy risks associated with the growing adoption of electronic information technologies by organizations. This report marked the first comprehensive study of the shift from traditional paper-based systems to electronic systems for the creation, storage, and retrieval of information. To mitigate these potential hazards, the HEW Report formulated a set of guidelines referred to as the "code of fair information practices", which is presently recognized as the Fair Information Practice Principles (FIPPs).

As implemented in the Privacy Act, the FIPPs allow individuals to-

- Determine what records pertaining to them are collected, maintained, used, or disseminated by an agency.
- Require agencies to procure consent before records pertaining to an individual collected for one purpose could be used for other incompatible purposes.
- Afford individuals a right of access to records pertaining to them and to have them corrected if inaccurate; and
- Require agencies to collect such records only for lawful and authorized purposes and safeguard them appropriately.

Exceptions from some of these principles are permitted only for important reasons of public policy. Judicial redress is afforded to individuals when an

agency fails to comply with access and amendment rights, but only after an internal appeals process fails to correct the problem. Otherwise, liability for damages is afforded in the event of a willful or intentional violation of these rights.

The Privacy Act was later modified by the Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507, extending the Privacy Act's FIPPs-based protections to computer-matching activities by agencies, with requirements for certain additional internal agency procedures. However, the original language of the Privacy Act, as drafted in 1974, has shown itself sufficiently flexible to adapt to those changes. More than any other law in the field, the Privacy Act has, to a remarkable extent, withstood the test of time.

B. The Computer Matching and Privacy Protection Act of 1988

The Computer Matching and Privacy Protection Act of 1988 amended the Privacy Act to add several new provisions. See 5 U.S.C. § 552a(a)(8) -(13), (e) (12), (o), (p), (q), (r), (u) (2018). These provisions add procedural requirements for agencies to follow when engaging in computer-matching activities, provide matching subjects with opportunities to receive notice and to refute adverse information before having a benefit denied or terminated, and require that agencies engaged in matching activities to establish Data Protection Boards to oversee those activities. These provisions became effective on December 31, 1989.

C. Health Insurance Portability and Accountability Act 1996 (herein after referred as HIPPA)

Before HIPPA, in 1850s the health insurance industry consisted of a handful of companies offering accident insurance. The industry expanded in the early 1900s due to the introduction of employer-sponsored plans, billions of employees' information is collected and stored. All the collected information stored and processed with the unmannered mechanism, because of the absence of regulations.

The federal government got involved in regulating the insurance industry in 1970 with the passage of Employee Retirement Income Security Act (ERISA). However, this Act only covered employer-sponsored and individually purchased health plans, while commercial for-profit group health plans were still governed by inconsistent state laws. So, this inconsistency of law impacts the rights of employees and creates issues during the changes of job without losing benefits. Many state laws also allowed group health plans to deny coverage, enforce higher deductibles, no security of information stored, or charge higher premiums for plan members with pre-existing conditions creating a "job lock" scenario in which many workers were stuck in jobs permanently.

To regulate the employee's insurance and the information of employes with one set of rules and regulations, the Healthcare Insurance Portability and Accountability Act (HIPAA) was passed on 21st august, 1996. A major goal of HIPPA is to assure that individuals health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and wellbeing. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing.

HIPPA covers the following(*HIPAA and Your Privacy Rights*, 1996):

- To Provide the ability to transfer and continue health insurance coverage for millions of American workers and their families when they change or lose their jobs.
- To reduce health care fraud and abuse.
- To mandates industry-wide standards for health care information on electronic billing and other processes; and
- To Requires the protection and confidential handling of protected health information.

Privacy and security Rule:

In response to the HIPAA mandate, Health, and Human Services (HHS) published a final regulation in the form of the Privacy Rule (the Security and Electronic Standards Security Rule) in December 2000, which became effective on April 14, 2001. This Rule sets national standards for the

protection of health information, as applied to the three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct certain health care transactions electronically. By the compliance date of April 14, 2003 (April 14, 2004, for small health plans), covered entities must implement standards to protect and guard against the misuse of individually identifiable health information. The Privacy Rule defined the term "Protected Health Information" (PHI) as "any information held by a covered entity which concerns health status, the provision of healthcare, or payment for healthcare that can be linked to an individual."

The Privacy Rule instructs "covered entities" (CEs) on how best to maintain the integrity of private data and stipulates the allowable uses and disclosures of identifiable health information. The Privacy rule also gave patients new rights over their healthcare data, including the right to obtain a copy of their health records, the right to amend healthcare records to correct errors, and the right to prevent details of private healthcare treatments from being disclosed to health insurers.

Enforcement Rule:

Despite the privacy and security risks that persist if healthcare organizations do not comply with HIPAA, many Covered entities (CEs) failed to implement compliance programs. This led to the introduction of the Enforcement Rule in 2006, which gave the Department of Health and Human Services the authority to enforce compliance with HIPAA and fine covered entities found not to follow the HIPAA Privacy and Security Rules. It also gave Health and Human Services (HHS) the right to pursue criminal charges against covered entities and individuals for serious violations of HIPAA Rules.

D. Health Information Technology for Economic and Clinical Health (HITECH) Act 2009

HITECH expands on the notions of privacy and security found in the Health Insurance Portability and Accountability Act of 1996, known as HIPAA. The HIPAA regulations, in brief, prohibit the disclosure of individually identifiable health information, otherwise known as protected health information or PHI, without the consent of the patient (or guardian or other

responsible person) except for three purposes: treatment, payment, or health care operations. HITECH mandates public notification of security breaches when "unsecure PHI" is disclosed or used for an unauthorized purpose. In general, the act requires that patients be notified of any breach of their data security, whether external or internal. If a breach affects 500 patients or more, then HHS must also be notified and the name of the institution where the breach occurred will be posted on the HHS web site. Under certain conditions, local media will also need to be notified. When a health care practice or organization implements an EHR system, the act gives patients in those practices (or third parties they designate) the right to obtain their PHI in an electronic format. This requirement is similar to state laws that mandate patients' access to their own paper medical records. In case of non-fulfilment of rules, civil penalties are mandatory if there is a violation due to willful neglect. For example, in situations in which a person is unaware of a violation (despite due diligence), the minimum penalty is $100 per violation, with a cap of $25,000 for violations of an identical requirement during a calendar year. If the violation is due to "willful neglect," however, the minimum penalty is $10,000 per violation, with a cap of $250,000 for violations of an identical requirement during a calendar year, and the maximum penalty is $50,000 per violation, with a cap of $1.5 million(Burde, 2011).

E. Amendment to HITECH 2021

The primary emphasis of the amendment lies in granting the Health and Human Services (HHS) Office for Civil Rights the authority to exercise discretion in abstaining from enforcement measures, lessening the severity of penalties for non-compliance with HIPAA, or shortening the duration of a Corrective Action Plan. This discretion is applicable when the party at fault for a data breach or any other security-related violation of HIPAA has successfully implemented a recognized security framework and consistently operated it for a period of twelve months prior to the incident.

Omnibus Final Rule:

In 2013, the most recent addition to HIPAA came into law, the Omnibus Final Rule. Though it did add much in the way of new legislation, it served to tighten

up the language of HIPAA and addressed many gaps in the original laws. For example, the Omnibus Final Rule stipulated that under HITECH requirements, all messages sent outside the CE's firewall must be encrypted.

The original HIPAA legislation was vague in its definitions, which the Omnibus Final Rule rectified. For example, the definition of "workforce" was changed to make it clear that the term includes employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or Business Associate, is under the direct control of the covered entity or Business Associate.

The Omnibus Final Rule also amended the Privacy and Security Rules. Patient records allowed to be held indefinitely, rather than the fifty years. The HITECH Act also increased the penalties for HIPAA violations to encourage compliance with HIPAA Rules.

F. Children's Online Protection Act (COPPA) 1998

The Children's Online Protection Act (COPPA) is a federal privacy law in the United States that was passed in 1998 and came into effect in 2000(*Overview: Children's Online Privacy Protection Act (COPPA)*, 2021). The main aim of this act, to protect privacy and personally identify information of children under the age of 13 who use online services. The law places rules on the use of data from and about children under 13 that are stricter than those governing data about older people and offers parents the ability to monitor and approve some of the information their children share.

COPPA adds another distinct layer of privacy regulation that companies that traffic in personally identifying information need to deal with. Some sites attempt to avoid complying with COPPA by simply banning young users altogether; other sites may not consider themselves to be appealing to the under-13 set and therefore not subject to COPPA's rules, but the FTC may take a different view based on a site's content. While the law originated in the early days of the Internet, it's even more important in the modern age of social media and programmatic ads(Fruhlinger, 2021).

G. General Data Protection Regulation (GDPR) 2018

The General Data Protection Regulation (GDPR), officially known as Regulation (EU) 2016/679, was implemented by the European Union (EU) on May 25, 2018, following its enactment into law in April 2016. The General Data Protection Regulation (GDPR) encompasses the processing of personal data and the unrestricted transfer of said data for an estimated population of 500 million individuals inside the European Union, in addition to Norway, Liechtenstein, and Iceland. The General Data Protection Regulation (GDPR) regulates the conduct of both organizations and individuals who assume the role of data controllers and processors in relation to personal data.

The General Data Protection Regulation (GDPR) was preceded by two significant directives pertaining to data protection. The initial document under consideration is the "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-border Flow of Personal Data"(often referred to as the OECD Recommendations on Protection of Privacy), which was established in 1980 by the Organization for Economic Cooperation and Development (OECD)(Daigle & Khan, 2020). The second directive referred to is the 1995 EU Data Protection Directive, which was developed based on the seven overarching principles outlined in the OECD Recommendations on the Protection of Privacy. The Directive was responsible for overseeing the management of personal data on the internet from 1995 until the implementation of GDPR in 2018(Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995).

H. California Consumer Privacy Act (CCPA) 2020

The California Consumer Privacy (CCPA) Act was the first US state privacy law, establishing consumer's rights and company responsibilities, and influencing subsequent legislation. The CCPA was passed in 2018 and came into effect on January 1st, 2020. It applies exclusively to consumers residing in California and regulates the protection of their personal data. This sweeping legislation creates significant new requirements for identifying, managing, securing, tracking, producing, and deleting consumer privacy information.

Rights of the consumer in CCPA are:

i. To know what personal information is collected about them.
ii. To know whether and to whom their personal information is sold/disclosed, and to opt-out of its sale.
iii. To access their personal information that has been collected.
iv. To have a business delete their personal information.
v. To not be discriminated against for exercising their rights under the Act

CCPA Covered:

The Act covers the Personal Information of all natural persons who are California Residents. The Act defines a "resident," as

(1) every individual who is in the State for other than a temporary or transitory purpose, and

(2) every individual who is domiciled in the State but is outside the State for a temporary or transitory purpose.

Restriction/Prohibition:

The CCPA prohibits selling personal information of a consumer under 17 without consent. Children aged 13-16 can directly provide consent. Selling personal information about a child under 13 requires parental consent. Importantly, protections provided by the US federal Children's Online Privacy Protection Act (COPPA) still apply on top of the CCPA's requirements.

Privacy Notices/Information Right:

CCPA requires very specific privacy notices as well as providing the right to opt out of the sale or use of personal information. Privacy notices need to inform consumers about what personal information categories will be collected and the intended use or purpose for each category. notices need to inform consumers about what personal information categories will be collected and the intended use or purpose for each category.

I. Cybersecurity Internet of Things Act (IoT) 2020

A universe of devices and technology has fallen into our laps at a speed that organizations struggle to manage effectively. And that boom in devices shows

no signs of stopping. In 2019, there were an estimated 9.9 billion Internet of Things (IoT) devices. By 2025, we expect 21.5 billion(Ingalls, 2021). As more information about IoT device vulnerabilities is published, the pressure on industry and government authorities to enhance security standards might be reaching a tipping point. For regularizing and improvement of the security for the IoT devices, the president signed the Cybersecurity IoT bill on 4th December 2020.

The main purpose of this bill is to support the growing market of IoT devices by providing cybersecurity. National Institute of Technology and Standards (NIST) published the minimum-security requirements and guidelines on vulnerability disclosures for IoT devices by March 4th, 2021.

When IoT device manufacturer can introduce the devices in the market, then the engineers need to follow these simple steps:

- Review NISTIR 8259 documents and compare the defined requirements with your IoT devices.
- Stay up to date on the National Institute of Standards (NIST) cybersecurity requirements.
- Review your company's current vulnerability disclosure policy (VDP).

Moreover, the standards may be probative of industry best practices against which private companies may be evaluated in reasonableness of security measures and may be used as a standard of care in IoT security. The IoT Act outlines a collaborative process whereby the NIST guidance is to be developed in consultation with public and private sector cybersecurity experts. To the greatest extent possible, the guidelines are to be aligned with industry best practices and are to be updated, at a minimum, every five years(Alvarez et al., 2020).

J. The Data Act 2022

The European Commission presented a proposal on 23 February 2022 for an EU regulation known as 'The Data Act', which aims to establish standardized regulations governing equitable access to and utilization of data. The objective is to eliminate obstacles that impede the ability of consumers and businesses to obtain data. This is particularly important given the rapid growth of data

generated by both humans and machines, which has become a crucial element for fostering innovation in businesses (such as algorithm training) and in public authorities (such as the development of smart cities, smart hospitals). The proposed legislation aims to establish standardized regulations pertaining to the sharing of data derived from the utilization of interconnected products or associated services, such as the internet of things and industrial machinery. Its primary objectives are to promote equity in data-sharing agreements and enable public sector entities to access enterprise-held data in cases of extraordinary necessity, such as during public emergencies.

5.4. Comparative Analysis

S. No	Point of Comparison	India	United States	Europe
1	**Rules, Regulation, Laws in related to 'Patient Privacy'.**	• After the judgment of justice in the K.S. Puttaswami case, the right to privacy is protected as a fundamental right under Article 21. • But under the umbrella term of '*Right to Privacy* there is nowhere specifically define the Right for the Patient Privacy.	• *The Privacy Act, 1974* was the first principal law that governs and regulates personal Information. • Later, in 1996 the Health Insurance Portability and Accountability (HIPPA) Act was enforced. Main aim to introduce HIPPA is protect the patient privacy (Subpart E-PRIVACY OF INDIVIDUALLY	• No Specific statue

			IDENTIFIABLE HEALTH INFORMATION of § 164.520 and § 164.522).	
2	**Protection of Electronic Medical Devices.**	• There is no specific provision that covers 'Electronic Medical Devices'. • The Drugs, Medical Devices and Cosmetics Bill, 2022 is not securing the electronic medical devices. • The medical devices rule, 2017 under the Drug and Cosmetic Act 1945 is only focusing on quality of the medical devices.	• In Medical Device Amendments to Food, Drug and Cosmetic act 1976 laid down the provision regarding the safety and efficacy of medical devices (Class II-Performance Standard) • Safe Medical Devices Act of 1990 and the Medical Device Amendments of 1992 cover the special provision related to 'Medical Device Tracking' (Section 3 (e)) and 'Medical Device Reporting System'(Section 2(b) (1) (A)). • In Radiation Control for Health and Safety Act 1968,	• No Specific Statue

			Section. 354 in declaration of purpose mentioned 'include the development and administration of performance of standards to control the emission electronic medical devices radiation and investigate the effects of radiation and control over them.'	
3.	**Rules/Regulation Pertaining to the regulation of Electronic Medical Record.**	• In Rule 9 (iv) of the Clinical Establishments (Central Government) Rules, 2012 covers only the maintaining patient record in Electronic Medical Records or Electronic Health Records. • In Electronic Health Record Standard 2016, covers only the goals/aim to introduce the Electronic Medical Record System.	• In HITECH Act, codifies a definition of 'Electronic Health Record in Section 42 U.S.C. 17921(5) • In 21st Century Cures Act, 'Section 4005 and Section. 11002'promotes and mandates the validation of EMR system. • Omnibus Final Rule 2013, set the limit for storing the patient data.	• No Specific statue.

			• Health Insurance Portability and Accountability Act 1996 (HIPAA) Rules is the first act that discuss and covers about the Electronic Medical Record (SUBPART E-PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION § 164.530 Administrative requirement).	
4.	**Provision for the Internet of Things/Artificial Intelligence based Medical Devices.**	• No specific statue	• Cybersecurity Internet of Things Act (IoT) 2020, introduced to force the IoT devices manufacturer and the government to enhance the security standard for regularizing the security of IoT devices.	• Data Act 2022, main aim to EU Data Act (COM (2022).
5.	**Provision with reference**	• There is no specific provision that is	• There is no Specific statue.	• In General Data

	to patient sensitive data: define/processing/transfer.	related to 'Patient sensitive data.' • The Information Technology (Reasonable Security Practices and Procedure and Sensitive Personal Data Information) Rules 2011, in Rule 3 Define sensitive personal data. This definition is given a broader sense.	• In HIPPA 1996, tries to cover sensitive data under the category of personal health information (PHI) in Subpart E (PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION) of HIPPA.	Protection Regulation (GDPR) 2018, Article 4(15) define 'data concerning health'. • For Processing of patient sensitive data, GDPR Article 5 and 9 covers principles for processing data. • Under GDPR, Article 44 and 45

				covers the transfer of data.
6	**Remedies/Penalties/Compensation if patient sensitive data breach.**	• No Specific Statue	• In HIPPA 1996 Subpart D- Imposition of Civil Money Penalties covers the remedies for the patient data breach. • Health Information Technology for Economic and Clinical Health Act 2009, discuss the provision for the penalties of patient data breach (Subtitle D- Privacy of Section 13404)	• In GDPR 2019, Article 83(4), 83 (5) and 83(6) discuss the penalties for the infringement of patient rights and breach of data.

5.5. Conclusion:

The healthcare industry has experienced a significant increase in the adoption of technology, leading to a transformative impact on the provision of patient care and management. A significant development in the field of healthcare is the extensive implementation of Electronic Health Records (EHRs), which serves to streamline the management of patient data and improve the coordination of care. Artificial Intelligence (AI) and Machine Learning (ML) are currently serving as significant contributors in the field of data analysis, facilitating the provision of individualized treatment plans and enhancing the

precision of diagnostic procedures. The utilization of Internet of Things (IoT) technology and wearable devices monitoring tools is enabling patients and healthcare practitioners to access real-time health data, hence simplifying proactive health management. The field of robotics has been instrumental in revolutionizing surgical procedures and enhancing patient care by facilitating precise and minimally invasive treatments. Although the technical breakthroughs offer unparalleled advantages, they also present issues pertaining to data privacy and ethical implications. The continuous use of technology in the healthcare sector demonstrates a dedication to optimizing operational effectiveness, promoting patient results, and adapting to the changing demands of the healthcare landscape. The integration of IoT and AI technology into the healthcare industry has presented a range of legal complexities that require thorough examination. One of the foremost considerations is to the preservation of data privacy and the safeguarding of patient's sensitive data. The integration of IoT and AI technology into the healthcare industry has presented a range of legal obstacles that require meticulous examination. One of the primary issues pertains to the safeguarding of data privacy and security.

The European Union (EU) and the United States have jointly undertaken measures to protect patient data within the healthcare industry, acknowledging the paramount significance of privacy and security. The General Data Protection Regulation (GDPR) in the EU serves as an extensive legislative framework that guarantees strong safeguards for the confidentiality and security of patient information. The GDPR puts rigorous obligations on healthcare providers and affiliated companies for the handling of personal data, including sensitive health information. The legislation provides individuals with precise rights to their data and mandates corporations to enforce rigorous security measures, acquire informed permission, and promptly disclose any instances of data breaches. Furthermore, the member states of the European Union have established independent national data protection authorities that are responsible for implementing this legislation and applying penalties in cases of non-compliance.

Patient data protection in the United States is managed by a comprehensive framework of federal and state rules, with the Health Insurance Portability and Accountability Act (HIPAA) serving as a fundamental pillar. The HIPAA creates a set of regulations that govern the safeguarding of confidential health data, referred to as Protected Health Information (PHI). Healthcare providers, along with other covered entities, are obligated to establish protective measures to preserve PHI and comply with stringent privacy regulations. The enforcement of compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the imposition of penalties for violations are carried out by the U.S. Department of Health and Human Services (HHS).

Globally, the EU and the U.S. have actively participated in cooperative endeavors aimed at enabling the secure movement of patient data across international boundaries. The EU-U.S. Privacy Shield, despite its invalidation in 2020, served as a framework intended to guarantee compliance of U.S. corporations with EU data protection regulations in their management of patient data. The ongoing conversations and discussions are focused on the establishment of new frameworks that attempt to ensure sufficient safeguards for the transmission of data across borders. Both the EU and the U.S. have underscored the significance of cybersecurity within the healthcare sector. In the context of healthcare delivery, the ongoing influence of technology necessitates the implementation of robust cybersecurity measures, the use of encryption technologies, and the promotion of awareness regarding the potential hazards associated with data breaches. These endeavors are essential elements within the overarching strategy aimed at safeguarding patient data. Finally, both the EU and the U.S. have exhibited a strong dedication to safeguarding patient data by implementing comprehensive legal structures, exercising regulatory supervision, and engaging in international partnerships. With the growing digitization of healthcare, these procedures aim to foster patient trust by guaranteeing the meticulous handling and protection of their sensitive health data.

India has the potential to gain substantial advantages by implementing optimal strategies for safeguarding patient data, as derived from Europe and the United States. The study has established comprehensive frameworks and regulatory

measures, exemplified by the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the United States, which impose stringent requirements on data privacy and security within the healthcare industry. By adhering to these established guidelines, India has the potential to augment the safeguarding of patient-sensitive information, so ensuring the preservation of confidentiality and privacy pertaining to individual's health data.

The GDPR, for example, places significant emphasis on key concepts such data minimization, purpose limitation, and the necessity for explicit agreement. This regulatory framework offers a holistic approach to the management of personal data. The implementation of such principles can facilitate the establishment of a robust framework for the responsible management of healthcare data in India. Furthermore, GDPR places significant importance on the principles of transparency and accountability. This necessitates that enterprises effectively disclose their methods of handling patient data and assume responsibility for their data processing activities. The implementation of transparency and accountability measures has the potential to enhance patient trust in the healthcare system of India.

In contrast, HIPAA is a regulatory framework that particularly centers its attention on the protection of health information within the United States. The severe standards pertaining to security measures, risk assessments, and breach notifications present in the context offer useful insights that can be utilized by India to enhance its healthcare data protection architecture. Drawing lessons from the United States experiences in managing electronic health records and telemedicine can assist India in proactively addressing potential issues and developing preventative strategies.

India has the potential to foster worldwide collaborations in healthcare research and innovation by incorporating the most effective approaches observed in Europe and the United States. Researchers and healthcare providers from the regions may exhibit a greater inclination to engage in collaborative efforts and exchange data if they possess a sense of assurance regarding India's commitment to upholding globally acknowledged data privacy standards.

Lastly, the adoption of proven methodologies and strategies employed in Europe and the United States has the potential to enhance India's healthcare data protection protocols. The alignment described not only serves to improve patient trust and privacy, but also establishes India as a responsible participant in the management of healthcare data. This positioning facilitates international cooperation and contributes to the progress of healthcare practices worldwide.

CHAPTER 6

CONCLUSION AND SUGGESTIONS

6.1. Conclusion

In conclusion, this Research has provided insights into significant factors affecting India's ability to build a robust framework for safeguarding patient data. This Research conducted a thorough review of the legislative framework in India, providing a comparative assessment of legislation in the European Union (EU) and the United States (US). The research findings validate the insufficiency of India's existing legal framework in effectively tackling the complexities presented by sophisticated healthcare technology, underscoring the imperative for the development of comprehensive legislation and regulatory measures.

The Research delves into the historical context of privacy, highlighting its ongoing importance in protecting personal boundaries. This Research explores the intricacies of the global healthcare industry, uncovering deficiencies in existing approaches and emphasizing the urgent requirement for innovative procedures. The incorporation of technology within the healthcare sector has a multitude of benefits, while concurrently raising legal considerations, namely pertaining to the safeguarding of data privacy and security.

This Research provides a critical evaluation of India's legal status, with a specific focus on the healthcare sector. It sheds light on ongoing concerns within this sector, including infrastructure limitations and regional discrepancies. The analysis of global models, particularly the General Data Protection Regulation (GDPR) in the European Union (EU) and the Health Insurance Portability and Accountability Act (HIPAA) in the United States (US), underscores the significance of strong legal structures in safeguarding the security of patient data. The importance of India's adoption of established

approaches from Europe and the US to improve its healthcare data protection measures is stressed.

The research highlights the pressing need for India to undertake legal reforms that are in line with internationally recognized best practices. By adopting this approach, India has the potential to not only effectively tackle existing issues pertaining to the safeguarding of patient data, but also establish itself as a conscientious contributor to international healthcare protocols. The report continues by advocating for the implementation of collaborative efforts, international collaborations, and the adoption of effective tactics witnessed in Europe and the US to promote the advancement of healthcare practices and the preservation of patient confidence and privacy in India.

The objective of this chapter is to incorporate the suggested recommendations into the existing legislative framework of India to effectively solve the gaps discovered by researchers in their comprehensive research findings. The Research has been systematically divided into six parts, each focusing on different aspects of privacy and the regulatory framework for protecting patients' data in India, the European Union (EU), and the United States (US). To achieve a full assessment of the research hypothesis, the researcher has purportedly structured the chapters in a manner that promotes a thorough understanding of the importance of strong rules, laws, and policies regarding the protection of patient data in India.

In this Research, the researcher conducts a comparative analysis between the existing legislation in India regarding Electronic Medical Records, Patient Sensitive Data, and upgraded Medical Devices, and the similar rules in the European Union and the United States. Upon the conclusion of the investigation, the researcher validates the findings by doing a comparative analysis using the data collected using the Likert scale 5.0 questionnaire approach.

After conducting a thorough analysis of many essential components of the proposed legislation, the researcher has concluded that the research hypothesis has been confirmed in a positive manner. The result is reflected considering the discussions offered throughout the Research. Without a doubt, one might argue that the existing legal framework in India does not

sufficiently handle the protection of patient data and the regulation of contemporary medical technology. In the following parts, the researcher concludes different attributes and proposed legislation that substantiate the researcher's conclusion pertaining to the hypothesis.

The notion of privacy possesses a profound historical lineage, originating from ancient societies in which individuals deliberately pursued seclusion and alone. Even within the communal living arrangements prevalent in early societies, individuals understood the importance of establishing personal boundaries and zones. During the historical era of ancient Rome, persons belonging to the upper echelons of society upheld the practice of reserving exclusive rooms within their residences, therefore underscoring the significance attributed to personal spatial demarcations and the protection of sensitive matters. The concept of privacy became increasingly interconnected with cultural, religious, and legal frameworks as societies faced various transformations. The preservation of privacy holds significant importance and serves as a vital mechanism for protecting the fundamental rights and dignity of persons within a given society. Privacy functions as a protective measure against unlawful encroachment into personal affairs, granting individuals the ability to maintain control and independence over their own existence. The establishment of trust between individuals and institutions, irrespective of their categorization as political, corporate, or social entities, is a fundamental component. The preservation of freedom of speech is contingent upon safeguarding privacy, as individuals are more inclined to partake in uninhibited self-expression when they feel secure within their personal domains. Furthermore, the concept of privacy plays a crucial role in creating an individual's sense of self and cultivating close interpersonal connections. The absence of guarantees about privacy may result in individuals displaying reluctance to engage in self-reflection and authentic self-disclosure, so impeding personal development and societal advancement.

In the initial stages of the research process, researchers employ the funnel down approach. The research commences by examining the historical context of privacy and underscores the continuing importance attributed to privacy throughout many historical periods, including ancient civilizations. The

concept of privacy has been extensively discussed in many legal rulings at both national and international levels. This discourse aims to explore the importance of privacy in various domains, including the confidentiality of personal correspondence, privacy within familial and relational contexts (such as married life), the protection of children's privacy, the confidentiality of telephonic conversations, and the safeguarding of medical records in the healthcare sector. The primary focus of this Research refers to the privacy within the healthcare sector, with an emphasis on the utmost importance of protecting patient confidentiality.

The healthcare industry functions on a global level, displaying a complex and interconnected system that surpasses the confines of individual nations. This network comprises a diverse range of people and incorporates multiple activities. At its core, the healthcare sector is driven by a steadfast commitment to providing medical services, promoting holistic well-being, and addressing global health challenges. This research aims to provide a comprehensive understanding of the operating mechanisms employed by both traditional and healthcare systems, together with an analysis of their distinct approaches to patient diagnosis Having reviewed the prior research it has become apparent that the methodologies and medical gadgets utilized in the healthcare industry demonstrate a multitude of deficiencies. The issues encompassed in this context are the assurance of patient medical information security in paper-based formats, as well as the precise translation of acquired numerical data into a chart or record. As a result, it is common for patients to navigate through an unstructured network of healthcare providers and services, resulting in the fragmentation of healthcare. The concern surrounding affordability has become a prominent problem considering the continuous increase in healthcare costs, leading to a significant economic burden on patients.

To effectively tackle the concerns, it is crucial to develop and execute innovative approaches and procedures. The lack of integration can lead to inefficiencies, duplication of testing, and insufficient coordination of comprehensive care. The researcher subsequently investigates the effects of technology adoption on traditional healthcare practices, specifically

highlighting its role in enhancing the efficiency of physicians in delivering patient care.

The Research unveiled that technology assumes a key function within the healthcare industry, demonstrating its efficacy and presenting innovative opportunities for advancement. Healthcare organizations are increasingly adopting emerging technologies, including Artificial Intelligence (AI), Blockchain, and the Internet of Things (IoT), which are widely present in various software and hardware solutions utilized in business. The widespread integration of various home medical devices, such as infrared thermometers and heart rate monitors, has been facilitated by the rapid expansion of modern technology in contemporary society. These devices have been utilized to measure important physiological parameters, including heart rate and body temperature. Within the realm of intelligent healthcare, individuals possess the capacity to transmit their physical health data, acquired through smart medical devices, to a medical professional or a self-service medical platform. This enables the procurement of specialized healthcare guidance.

The exponential advancement of technology has surpassed the concurrent establishment of regulatory frameworks, resulting in a scarcity of rules and legislation to adequately address the developing issues and complexities. The researcher highlights the need and necessity of establishing a regulatory framework for smart devices in the healthcare sector.

The emergence of the healthcare industry has undoubtedly brought about a significant transformation in the process of identifying and treating patients, leading to several benefits. However, this development has also given rise to a wide range of legal issues and challenges. The issue of data privacy and security has received considerable attention in academic discourse. The increased prevalence of electronic storage and communication of sensitive patient information has led to a heightened vulnerability to data breaches, so placing healthcare companies at risk of substantial legal consequences and jeopardizing patient confidentiality. Similarly, manufacturers of intelligent devices are obligated to adhere rigorously to tough regulations that mandate the need for accessing the private domain of all gadgets. The legal system must develop novel legislation and policies that effectively reconcile the

emergence of innovative technologies such as the IoT and AI, particularly within the healthcare sector. The protection of patient-sensitive data is of utmost importance in the healthcare industry due to several critical concerns. The key consideration revolves around the protection of patient privacy and confidentiality. Medical records may contain very sensitive information related to an individual's health status, medical history, and treatment measures. The improper acquisition of this data has the capacity to violate a patient's fundamental right to privacy, thereby eroding the trust placed in healthcare professionals and potentially discouraging individuals from seeking necessary medical care.

Moreover, the principal research inquiry of this Research regarding the issues and obstacles that exist in the healthcare industry following the implementation of technological advancements. The resolution of these concerns and challenges necessitates the establishment of legislation and regulations pertaining to the healthcare sector.

Further to analyse the awareness and the knowledge about privacy and data protection rights, an Empirical study was conducted to check the level of agreements among the various stakeholders which includes public, legal academician, advocates, and Doctors. Participants universally acknowledge the significance of privacy in family dynamics, interpersonal connections, marital bonds, and individual personal boundaries. The fragility of paper-based medical data has raised significant concerns, leading to a strong demand for technological developments. In India, 90.8% of individuals support the use of Electronic Medical Record (EMR) systems. A multitude of viewpoints arise about topics such as data security, Internet of Things (IoT), artificial intelligence (AI), and the efficacy of legislation, underscoring the intricate nature of views.

Subsequently, the researcher addressed the legal stance of India in addressing data privacy concerns pertaining to Electronic Medical Records (EMR) within the healthcare industry. The healthcare system in India demonstrates a dual structure, including of both governmental and private healthcare providers. Public healthcare controlled by the government aims to cater to the healthcare needs of the overall population, particularly emphasizing rural areas that lack

adequate access to healthcare services. However, the healthcare industry continues to face ongoing challenges, such as inadequate infrastructure, a shortage of healthcare professionals, and disparities in access based on geographic location. Prominent trends observed in the domain of technology encompass the extensive use of electronic health records, the application of telemedicine, the incorporation of Artificial Intelligence, and the growth of the Internet of Things. The COVID-19 pandemic has underscored the critical need for a robust healthcare infrastructure, leading to efforts aimed at bolstering capacity and executing vaccination campaigns.

Significant changes have been made through the developments in the health care sector but on the other hand the sector is still facing many challenges. One of the major challenges revolves in the ethical and legal ramifications linked to emerging technologies, such as genetic manipulation and artificial intelligence, within the domain of medical diagnosis and treatment. The contemporary era of networked health systems and electronic health records has intensified the complexity around patient privacy, patient data storage, inter-state movement of patient data, and data security. To address these challenges in a comprehensive manner, it is crucial to cultivate a collaborative effort that encompasses healthcare experts, policymakers, and technological innovators. The implementation of a collaborative strategy is of utmost importance to guarantee that advancements in healthcare result in improved patient outcomes, while also preventing the worsening of pre-existing disparities in healthcare access and quality. The existing legislation in India concerning the preservation and security of patient data, regulations for Electronic Medical Record Systems, and the smart medical device system is deemed inadequate. There is a compelling need for a comprehensive framework of legislation that oversees the burgeoning domain of medical devices, together with regulations concerning the protection of patient's data. During the era characterized by rapid technological progress, the healthcare sector has experienced the incorporation of advanced medical devices. To attain a cohesive fusion of law and technology, it is crucial to undertake the endeavor of modifying or revising prevailing legal structures by incorporating exemplary approaches from the European Union and the United States.

The hypothesis that has been substantiated and validated through the examination and analysis of the present Indian legal system is as follows: 'The current legal framework in India is inadequate in addressing the legal challenges arising from the integration of advanced technology in the Healthcare Sector.'

The European Union (EU) and the United States (US) have implemented laws to protect the well-being of patients in response to the fast-paced progress in technology. Both regions have established legislative frameworks that control the utilization of modern medical technologies, such as the Internet of Things (IoT) and Artificial Intelligence (AI). Nevertheless, significant disparities can be observed in the categorization of patient data and the procedures employed for processing prescribed data. The EU, via the General Data Protection Regulation (GDPR), guarantees a comprehensive legislative framework that prioritizes strong steps to maintain patient data confidentiality and security. The GDPR places strong obligations on healthcare organizations, confers unique data rights to individuals, and mandates strict security measures and timely reporting of data breaches.

Patient data protection in the United States is regulated by an intricate framework of federal and state legislation, including the Health Insurance Portability and Accountability Act (HIPAA). HIPAA mandates regulations for safeguarding and securing confidential health data, necessitating healthcare providers to enforce measures to preserve Protected Health Information (PHI) and comply with stringent privacy regulations. The Department of Health and Human Services (HHS) is responsible for supervising the implementation of regulations and imposing sanctions for failure to comply.

The EU and the US have worked together on a worldwide scale to enable safe and efficient transmission of patient data across borders. This collaboration is demonstrated by efforts such as the EU and U.S. Privacy Shield, which was declared illegal in 2020. Current deliberations center on the creation of novel mechanisms to guarantee the safeguarding of data during international transfers. Both areas prioritize cybersecurity and acknowledge the importance of robust procedures, encryption technologies, and understanding of the hazards related to data breaches in the healthcare sector.

India can derive advantages by incorporating elements from these frameworks. The GDPR's focus on data minimization, purpose limitation, express consent, openness, and responsibility offers a comprehensive framework for ethical management of healthcare data. India's healthcare data protection system can be enhanced by using the useful insights provided by HIPAA, which emphasizes security protocols, risk assessments, and breach notifications. India may cultivate global alliances by adopting successful approaches witnessed in Europe and the US, instilling trust in globally acknowledged data privacy norms, and promoting cooperation in healthcare research and innovation.

In conclusion, the implementation of established methods and techniques utilized in Europe and the United States holds the capacity to augment India's healthcare data protection measures. This shows that it will not only enhances patient trust and privacy, but also positions India as a conscientious contributor in healthcare data management. This strategic placement enables global collaboration, thereby making substantial contributions to the advancement of healthcare measures on a global scale.

6.2. Recommendations

The Indian government is being pushed to implement comprehensive measures to bolster data privacy and cybersecurity, in accordance with global norms. It is essential to acknowledge the "Right to Data Protection" as a basic right in Article 21 of the Constitution to protect personal data from illegal access and use. It is suggested that amendments be made to the IT Act 2000, namely in Chapter V, to provide a precise definition for "Sensitive Data" and provide explicit protocols for the protection and transmission of Electronic Medical Records (EMRs).

To comply with international data privacy regulations, particularly GDPR, it is imperative for the government to establish rigorous criteria for managing confidential information. Enhancing accountability and promoting transparent data handling methods can be achieved by implementing fines for data breaches involving sensitive information and establishing a supervisory body like GDPR's regulatory body. Moreover, it is crucial to bifurcate the

meaning of 'Sensitive Personal Data under SPDI standards to distinguish between financial and patient data.

It is recommended to enhance Rule 7 of the IT Rules, 2011, to facilitate the secure transmission of sensitive personal information to foreign countries, in accordance with the criteria set by GDPR. Within the field of medical devices, it is crucial to establish clear definitions for smart medical devices, implement privacy by design principles to protect user information, and address jurisdictional considerations in privacy agreements. The government should implement rigorous processing criteria, incorporating pseudonymization methods recommended by ENISA, and create a specialized organization for safeguarding network and information security, leveraging ENISA's exemplary approaches.

Organizations must implement secure means for storing patient data in accordance with HIPAA rules, while also completing comprehensive security assessments. It is crucial to include explicit clauses in the Electronic Health Record Standard 2016 to guarantee online accessibility, authority over data exchange, and strong security measures. Online access, confidentiality during foreign data transfers, and compliance with Indian data protection standards should be granted as rights to citizens and healthcare providers.

It is highly advisable to implement the Digital Information Security in Healthcare Act (DISHA), which will create a "National Digital Health Authority" responsible for full regulation of electronic health data. Considering the IoT Cybersecurity Improvement Act of 2020, it is advisable for India to contemplate implementing comparable legislation that sets forth fundamental security prerequisites for IoT devices, with a focus on security protocols, transparency, and collaborations between the public and private sectors. The purpose of these proposals is to strengthen data protection, cybersecurity, and privacy in the changing digital environment.

A. Constitution of India

i. Data Protection as a Fundamental Right:

Protecting personal data has become essential to maintaining individual liberty and privacy in a time when information travels quickly and freely across borders. It is necessary to incorporate the "Right to Data Protection" as

a fundamental right in Article 21 of the Indian Constitution. This recognition emphasizes the inherent importance of personal information and the requirement for strict mechanisms to govern its collection, processing, and dissemination. Every individual possesses a right to safeguard their personal data from unauthorized utilization by private entities without their explicit consent.

B. IT Act 2000 (amendment in 2008)

i. Definition of Sensitive Data

In Chapter I of the Information Technology Act 2000, the definition of Sensitive Data that includes patient data generated by any electronic or any Internet connected medical devices needs to be incorporated or added. Definition of *'data' in Section 2(o)*(*Section 2 in The Information Technology Act*, 2000) is the only definition that does not give clarity on the other type of data. So, the specific definition of sensitive needs to be prescribed.

ii. Need of Amendment in IT Act as to Secure Electronic Record

Chapter V of Information Technology (IT) Act 2000 deals with the 'Secure Electronic Records (Section 14(*Section 14 in The Information Technology Act*, 2000)) and Secure Electronic Signature (Section 15(*Section 15 in The Information Technology Act*, 2000))'. The definition or the concept of Electronic Medical Record (EMR) should be added. The EMR should include patient data (sensitive data) that is generated using electronic devices as well as any Internet used medical devices.

Section 16(*Section 16. Security Procedures and Practices*, 2000) of the IT Act need to be amended as to specific procedures and guidelines for securing or keeping patient's data and the practices to transfer or share the patient EMR. All organizations need to follow the rules and guidelines set under the security procedure.

iii. Processing of Sensitive Data

It is recommended that the government sets thorough standards for handling sensitive data, with a focus on adhering to the legitimate grounds set forth in Article 6 of the General Data Protection Regulation (GDPR). This involves making sure that data privacy laws are followed, stressing the need of processing for contractual responsibilities, and getting explicit and affirmative

agreement. To further encourage data privacy and protection culture, it is suggested that individuals be kept informed in a clear and open manner about how their data is processed.

iv. Punishment for violation of Sensitive Data

It is suggested that the Information Technology Act, 2008 be revised to include specific penalties for data breaches involving sensitive information in Chapter XI (Offences). The government should penalize organizations or authorities that willfully or negligently do not adhere to data management legislation in accordance with international standards, especially Article 39(1)(b) of the General Data Protection Regulation (GDPR) 2016.

Additionally, it is worth considering implementing sanctions for instances when sensitive data is not processed in accordance with the methods specified in Article 6 of the GDPR. According to Article 83(4) of the GDPR, administrative fines of up to 10,000,000 EUR or, for entities, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, should be instituted to ensure a robust enforcement mechanism. This strategy would help promote appropriate data management within the legal framework and discourage unlawful data processing.

v. Establish authority where the user report in case of sensitive data breach

To handle data breaches and protect the rights of individuals whose sensitive data has been exposed, India should set up a specialized supervisory body. India should think about creating a similar regulatory body to the one that the European Union's General Data Protection Regulation (GDPR) has in place, since Article 33(1) of that regulation requires the presence of such bodies.

To provide a quick and efficient response to limit the impact on impacted individuals, the supervisory authority should be empowered to accept and investigate allegations of data breaches. Those responsible for breaches of sensitive data should be held accountable by this institution, which should have the power to levy penalties and enforce corrective measures.

In addition to better safeguarding people's data privacy, establishing such a supervisory authority will give users a legal framework to pursue remedies in case of a data breach. A more trustworthy digital ecosystem and more

responsible data handling practices from businesses dealing with sensitive information can be achieved by creating transparent reporting and remedy channels.

C. SPDI Rule 2011

i. Bifurcation in the definition of 'Sensitive Personal Data'

In Rule 3 of SPDI rules, 2011, there is need for bifurcation of the definition of 'Sensitive personal data or information'. This definition is a combination of financial data and the sensitive data of patients. The importance and relevance of sensitive data and financial data are different, so, there should be two different definitions required So, there should be two different definitions required for sensitive data and financial data that is also called critical data.

ii. Transfer of Sensitive Data in third countries or international organization

We urge you to revise Rule 7 of the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 so that the rules governing the transfer of sensitive personal information to foreign countries are strengthened. To be in step with global norms and to make sure sensitive data is transferred securely, India should include criteria like the ones in GDPR (General Data Protection Regulation) Articles 45 and 46.

In particular, the security of patient-sensitive data should be a primary concern when evaluating the receiving country's data protection measures. The third country's security measures, including its laws and regulations, should be considered in this evaluation.

For a more comprehensive and specific approach to the transfer of sensitive personal data, India can improve its data protection legislation by adding these extra requirements. Taking this measure would help ensure the safety and privacy of people's data when it is transported across borders, particularly when it comes to sensitive health information.

D. Medical Devices Rules 2017

i. Smart Medical Devices

In the Medical Devices Rules 2017(*The Medical Devices Rules*, 2017), there is need to add the definition of smart medical devices with the electronic

medical devices. It includes the devices which can be used through any wireless network like Bluetooth, WI-FI or any Internet.

ii. Privacy by design of Medical Device

The Indian government should revise its laws regarding the production of medical devices so that patient's privacy is protected even when these devices are being developed. These provisions should handle the collection, processing, and transmission of user data by medical devices, taking a cue from Article 25 of the General Data Protection Regulation (GDPR) 2016. Furthermore, it is important that the privacy agreements clarify the jurisdictional aspects in the case of accidents or data breaches caused by these medical devices and offer an explicit explanation of the data security measures that these devices use.

The legislation would accomplish two goals: first, it would make sure that customers know how their data is handled by medical devices; and second, it would set a standard for manufacturers to make privacy and security their top priorities when they are designing their products. This foresight promotes a culture of accountable data management in healthcare technology development and is in line with worldwide standards.

In addition, users will have a better grasp of their legal options and the relevant legal framework in the event of any unexpected circumstances thanks to the inclusion of jurisdictional facts. Data privacy and security are paramount in the healthcare IT world, and this suggestion is an effort to boost consumer trust in medical device use.

E. Processing, Securing, Storage and transferring of Patient Sensitive Data

i. Secure Processing techniques for protecting patient sensitive data

For the protection of sensitive patient data, the Indian government must immediately institute stringent processing standards. These rules need to be all-encompassing and establish very high criteria that any company or individual handling this kind of data must meet. The goal is to provide a consistent and strong system to protect the privacy and integrity of patient data during processing.

Adopting pseudonymization techniques and best practices, as proposed by the European Union Agency for Cybersecurity (ENISA), will greatly increase security measures in India. India can take advantage of globally accepted standards for the efficient pseudonymization of patient-sensitive data by adopting ENISA's recommendations. By implementing this measure, the data is further safeguarded from potential illegal access or accidental disclosure.

Improving the entire security and privacy landscape for patient-sensitive information is crucial, and this proposal highlights the need of harmonizing India's data processing methods with worldwide cybersecurity standards. It is recommended that these rules be revised and updated on a regular basis to keep up with the ever-changing cybersecurity risks and healthcare technology developments.

ii. Secure Network and Information security

It is suggested that India establish a specific entity to guarantee the safety of networks that allow for the transfer of data, particularly data that is personal or identifiable to individuals. The state must take the initiative to secure these networks because of the widespread usage of internet platforms, Wi-Fi systems, and Bluetooth for the exchange of medical records amongst parties including hospitals, patients, and doctors.

India may learn a thing or two about network and information security from the EU's approach and maybe even implement some of the EU's best practices. When it comes to advocating for strong cybersecurity measures for information and network systems, the European Union Agency for Cybersecurity (ENISA) has proven to be an expert. India can make its healthcare data exchange networks more secure and less vulnerable to hacking, data breaches, and other cyber threats by adopting these best practices.

Healthcare information systems in India would be much better protected if this kind of organization were to be set up and if ENISA's best practices were to be implemented. These practices cover all bases when it comes to risk management, with a focus on cybersecurity risk identification, assessment, and mitigation. To effectively handle cyber incidents, ENISA emphasizes the need of strong incident response and management processes and encourages

enterprises to establish transparent protocols and communication plans. To keep up with the constantly changing technology world and make sure these security measures are effective, it is vital to regularly analyze, update, and collaborate with relevant stakeholders.

iii. Storage of Patient sensitive data

Organizations that are responsible for keeping patient information should implement a safe method of storing it in conformity with the regulations set out in § 160.516(Office of Civil Rights, 2013) of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. We advise conducting a thorough security Research before ordering companies to install security measures under the HIPAA Security Rule. The purpose of this examination is to find any weak spots or dangers that could compromise the safety of patient's personal information.

Secure storage and transmission protocols should be implemented by covered entities to meet the security requirements. Organizations should use secure servers, encrypt data at rest and in transit, and take other precautions to improve the security of patient-sensitive information; however, HIPAA does not mandate a particular technology. This method is in line with the dedication to preventing unwanted access to a patient's personal information and is in accordance with the security standards set out by HIPAA.

A strong security posture requires regular risk assessments, the use of data security best practices, and keeping up with changes to HIPAA laws. To make sure they're always following HIPAA rules, organizations can investigate official materials offered by the US Department of Health and Human Services (HHS) and talk to lawyers who focus on healthcare law.

iv. Secure Access to Health Data

The below part needs to be inserted in standard of Electronic Health Record Standard 2016 of India. The state should ensure:

- Their citizens and their healthcare providers have online access to their Electronic Health Records
- Citizens can decide with whom and to what extent they are going to share their health data.

- Registration and verification of any processing of health data for the purpose of auditing the access to and exchange of electronic data records.
- Technical and organizational security of electronic health record systems, particularly by measures which also involve protection against unauthorized or unlawful processing, and against accidental loss, damage, or destruction.
- Continuity and availability of EHRS to guarantee continuity of care.

v. Right to access and exchange of patient sensitive data outside India:

The citizen of India and their respective healthcare providers should be provided with right to:

- online access to their Electronic Health Record.
- confidentiality of patient sensitive data in case of transferring of patient data outside India
- patient have right to ensure that the processing of his/her data by the other country is complies with the data protection rules set by India.
- to get clarity on the jurisdiction in case of patient data breach by the foreign country during transfer, store, or process of patient data.

F. Proposals in General

The Government of India must adopt the ***Digital Information Security in Healthcare Act (DISHA)***. DISHA is a central organization known as the "National Digital Health Authority" that was established by an Act of parliament. It serves as a legislative authority with the purpose of promoting and adopting e-Health standards, ensuring privacy and security measures for electronic health data, and regulating the storage and interchange of Electronic Health Records.

G. Proposal to enact specific IoT Cybersecurity Improvement

It is highly recommended that India thinks about passing a law like the Internet of Things Cybersecurity Improvement Act of 2020 that the US passed. Establishing thorough rules and regulations to guarantee the greatest level of security in the IoT landscape is the principal goal of this law, which aims to create baseline security requirements for Internet of Things (IoT)

devices. The government should have broad power under the new law so that it can effectively oversee and supervise everything.

The proposed legislation should incorporate the U.S. Act's requirement that federal agencies follow certain security protocols when acquiring Internet of Things (IoT) devices. The capacity to receive security updates, the use of safe development approaches, and the lack of known vulnerabilities should all be part of these requirements.

The proposed laws should stress that manufacturers must reveal the cybersecurity capabilities of their Internet of Things devices in order to promote openness and transparency during the procurement process. Furthermore, it should promote the implementation of synchronized disclosure initiatives, guaranteeing that security experts can disclose vulnerabilities without facing legal consequences. In order to build a strong framework, the laws should push for the adoption of best practices and standards for Internet of Things security that are acknowledged by the industry.

Proactively addressing the ever-changing vulnerabilities in the IoT ecosystem requires legislation that prioritizes secure development methods, regular update capabilities, and openness. By establishing baseline standards and encouraging public-private partnerships, this law aims to strengthen the security and reliability of the IoT ecosystem. To help create a more secure Internet of Things, it is critical that companies and manufacturers follow these regulations.

REFERENCES

- Adeleke, I. T., Adesubomi Erinle, S., Ndana, A. M., Anamah, T. C., Ogundele, O. A., & Aliyu, D. (2014). Health Information Technology in Nigeria: Stakeholders' Perspectives of Nationwide Implementations and Meaningful Use of the Emerging Technology in the Most Populous Black Nation. *Http://Www.Sciencepublishinggroup.Com*, *3*(1–1), 17. https://doi.org/10.11648/J.AJHR.S.2015030101.13
- Adler, K. (2004). Why it's time to purchase an electronic health record system. *Undefined*.
- *Advancements in Healthcare Technology - Benefits for Today's Healthcare Students*. (2022). https://americancareercollege.edu/pulse/health-e-news/advancements-in-healthcare-technology-benefits-for-todays-healthcare-students.html#
- Agrawal, A., Gans, J. S., & Goldfarb, A. (2018). Exploring the Impact of Artificial Intelligence: Prediction Versus Judgment. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3177467
- Ahmad, M., Sadiq, S., Abdulmajid, A., & Saleh, A. (2020). *Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID- 19 . The COVID-19 resource centre is hosted on Elsevier Connect , the company ' s public news and information . January*.
- *AIIMS cyber attack: eHospital data restored, details of 3 crore patients still at risk amid Rs 200 cr ransom reports*. (2022, November 30). https://www.dnaindia.com/india/report-aiims-cyber-attack-ehospital-data-restored-details-of-3-crore-patients-still-at-risk-amid-rs-200-cr-ransom-3006763
- Aldeer, M., Javanmard, M., & Martin, R. P. (2018). A Review of Medication Adherence Monitoring Technologies. *Undefined*, *1*(2), 1–27. https://doi.org/10.3390/ASI1020014
- Ali, Z., Hossain, M. S., Muhammad, G., & Sangaiah, A. K. (2018). An

intelligent healthcare system for detection and classification to discriminate vocal fold disorders. *Future Generation Computer Systems*, *85*, 19–28. https://doi.org/10.1016/J.FUTURE.2018.02.021

- Allen, A. L. (2000). Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm. *Connecticut Law Review*, *32*(3), 861–875.
- Alpert, J. (2016). The electronic medical record in 2016: Advantages and disadvantages. *Digital Medicine*, *2*(2), 48. https://doi.org/10.4103/2226-8561.189504
- Alrizq, M., Solangi, S. A., Alghamdi, A., Nizamani, M. A., Memon, M. A., & Hamdi, M. (2021). An architecture supporting intelligent mobile healthcare using human-computer interaction HCI principles. *Computer Systems Science and Engineering*, *40*(2), 557–569. https://doi.org/10.32604/CSSE.2022.018800
- Alsubaei, F., Abuhussein, A., Shandilya, V., & Shiva, S. (2019). IoMT-SAF: Internet of Medical Things Security Assessment Framework. *Internet of Things (Netherlands)*, *8*(October). https://doi.org/10.1016/j.iot.2019.100123
- Alsubaei, F., Abuhussein, A., & Shiva, S. (2017). Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. *Proceedings - 2017 IEEE 42nd Conference on Local Computer Networks Workshops, LCN Workshops 2017*, *6*, 112–120. https://doi.org/10.1109/LCN.Workshops.2017.72
- Alvarez, D. K., Bower, E., Gray, E. P., Borden, R. M., & Ducich, S. (2020). *IoT Cybersecurity Improvement Act of 2020*. www.willkie.com.
- America, I. of M. (US) C. on Q. of H. C. in, Kohn, L. T., Corrigan, J. M., & Donaldson, M. S. (2000). *COMMITTEE ON QUALITY OF HEALTH CARE IN AMERICA*. https://www.ncbi.nlm.nih.gov/books/NBK225176/
- *American Nurses Association*. (n.d.). Retrieved December 7, 2022, from https://www.nursingworld.org/ana/
- Anand, A., Rani, S., Anand, D., Aljahdali, H. M., & Kerr, D. (2021). An efficient CNN-based deep learning model to detect malware attacks (CNN-DMA) in 5G-IoT healthcare applications. *Sensors*, *21*(19). https://doi.org/10.3390/s21196346

- Ananthi, J. V., & Jose, P. S. H. (2021). Implementation of IoT and UAV Based WBAN for healthcare applications. *Proceedings of the 3rd International Conference on Inventive Research in Computing Applications, ICIRCA 2021*, 37–42. https://doi.org/10.1109/ICIRCA51532.2021.9545052
- Anderson, G., of Health Policy, P., Health Johns Hopkins Bloomberg, I., Horvath, J., Knickman, J., Colby, D., Program Officer Stuart Schear, S., & Jung, M. (2002). *Partnership for Solutions would like to thank the following people for their contributions to this book: Principal Investigators Chronic Conditions: Making The Case for Ongoing Care*. www.partnershipforsolutions.org
- Anstey, P. R. (2011). John Locke and Natural Philosophy. *John Locke and Natural Philosophy*, 1–264. https://doi.org/10.1093/ACPROF:OSO/9780199589777.001.0001
- Apthorpe, N., Reisman, D., & Feamster, N. (2017). *A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic*. http://arxiv.org/abs/1705.06805
- Armgarth, A., Pantzare, S., Arven, P., Lassnig, R., Jinno, H., Gabrielsson, E. O., Kifle, Y., Cherian, D., Arbring Sjöström, T., Berthou, G., Dowling, J., Someya, T., Wikner, J. J., Gustafsson, G., Simon, D. T., & Berggren, M. (2021). A digital nervous system aiming toward personalized IoT healthcare. *Scientific Reports*, *11*(1), 1–11. https://doi.org/10.1038/s41598-021-87177-z
- *Article 21: Protection of life and personal liberty* . (n.d.). Constitutionofindia. Retrieved February 5, 2024, from https://www.constitutionofindia.net/articles/article-21-protection-of-life-and-personal-liberty/
- *Article 25: Right to Adequate Standard of Living*. (1948). https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23871&L
- Asplund, M., & Nadjm-Tehrani, S. (2016). Attitudes and Perceptions of IoT Security in Critical Societal Services. *IEEE Access*, *4*, 2130–2138. https://doi.org/10.1109/ACCESS.2016.2560919

- Balasubramanian, V., & Jolfaei, A. (2021). A scalable framework for healthcare monitoring application using the Internet of Medical Things. *Software - Practice and Experience*, *51*(12), 2457–2468. https://doi.org/10.1002/spe.2849
- Bennett, C. J. (Colin J. (1992). Regulating privacy : data protection and public policy in Europe and the United States. *Cornell University Press*, 263.
- Berberich, M., & Steiner, M. (2016). Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers? *European Data Protection Law Review (EDPL)*, *2*. https://heinonline.org/HOL/Page?handle=hein.journals/edpl2&id=448&div=&collection=
- Berg, M. (2001). Implementing information systems in health care organizations: Myths and challenges. *International Journal of Medical Informatics*, *64*(2–3), 143–156. https://doi.org/10.1016/S1386-5056(01)00200-3
- Bharadwaj, S. A., Yarravarapu, D., Reddy, S. C. K., Prudhvi, T., Sandeep, K. S. P., & Reddy, O. S. D. (2017). Enhancing healthcare using m-Care box (Monitoring non-compliance of medication). *Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017*, 352–356. https://doi.org/10.1109/I-SMAC.2017.8058370
- Bhardwaj, N. (2022). *An Overview of India's Healthcare Ecosystem*. https://www.india-briefing.com/news/indias-healthcare-ecosystem-key-segments-market-growth-prospects-26225.html/
- *Big Brother Is Us - The New York Times*. (n.d.). Retrieved July 14, 2022, from https://www.nytimes.com/1996/09/29/magazine/big-brother-is-us.html
- Blendon, R. J., DesRoches, C. M., Benson, J. M., Brodie, M., & Altman, D. E. (2001). Americans' views on the use and regulation of dietary supplements. *Archives of Internal Medicine*, *161*(6), 805–810. https://doi.org/10.1001/ARCHINTE.161.6.805
- Bodkhe, U., & Tanwar, S. (2021). Secure data dissemination techniques for IoT applications: Research challenges and opportunities. *Software* -

Practice and Experience, *51*(12), 2469–2491. https://doi.org/10.1002/spe.2811

- Boeldt, D. L., Wineinger, N. E., Waalen, J., Gollamudi, S., Grossberg, A., Steinhubl, S. R., McCollister-Slipp, A., Rogers, M. A., Silvers, C., & Topol, E. J. (2015). How Consumers and Physicians View New Medical Technology: Comparative Survey. *Journal of Medical Internet Research*, *17*(9), e215. https://doi.org/10.2196/JMIR.4456
- Bondre, A., Pathare, S., & Naslund, J. A. (2021). Protecting Mental Health Data Privacy in India: The Case of Data Linkage With Aadhaar. *Global Health: Science and Practice*, *9*(3), 467. https://doi.org/10.9745/GHSP-D-20-00346
- Boumehrez, F., Hakim Sahour, A., & Doghmane, N. (2021). Telehealth caFarouk Boumehrez, A. Hakim Sahour & Noureddine Doghmane, Telehealth care enhancement using the internet of things technology. *Bulletin of Electrical Engineering and Informatics*, *10*(5), 2652–2660. https://doi.org/10.11591/eei.v10i5.2968
- Brown, S. (2023). *What is Sensitive Data?* . https://www.strongdm.com/blog/sensitive-data
- Buntin, M. B., Burke, M. F., Hoaglin, M. C., & Blumenthal, D. (2011). The benefits of health information technology: a review of the recent literature shows predominantly positive results. *Health Affairs (Project Hope)*, *30*(3), 464–471. https://doi.org/10.1377/HLTHAFF.2011.0178
- Burde, H. (2011). The HITech act: An overview. *Virtual Mentor*, *13*(3), 172–175. https://doi.org/10.1001/VIRTUALMENTOR.2011.13.3.HLAW1-1103
- CAHAL, M. F., & CADY, E. L. (1962). Right of privacy. *Gp*, *26*(1), 176–177. https://doi.org/10.4324/9780203144589-15
- Cahn, N. R. (1998). Models of Family Privacy. *George Washington Law Review*, *67*. https://heinonline.org/HOL/Page?handle=hein.journals/gwlr67&id=1235&div=61&collection=journals
- Cain, R. M., Chike, C. P., AboBakr, A., Azer, M. A., Baldini, G., Botterman, M., Neisse, R., Tallacchini, M., Jamil, D., Khan, M. N. A.,

Duraiswami, D. R., Hornberger, R. C., Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2021). IoT privacy and security: Challenges and solutions. *Applied Sciences (Switzerland)*, *11*(1), 1–17. https://doi.org/10.1080/19393555.2020.1797948

- Calvillo-Arbizu, J., Román-Martínez, I., & Reina-Tosina, J. (2021). Internet of things in health: Requirements, issues, and gaps. *Computer Methods and Programs in Biomedicine*, *208*, 106231. https://doi.org/10.1016/j.cmpb.2021.106231
- Castiglione, A., Umer, M., Sadiq, S., Obaidat, M. S., & Vijayakumar, P. (2021). The Role of Internet of Things to Control the Outbreak of COVID-19 Pandemic. *IEEE Internet of Things Journal*, *8*(21), 16072–16082. https://doi.org/10.1109/JIOT.2021.3070306
- Channa, A., Popescu, N., Skibinska, J., & Burget, R. (2021). The rise of wearable devices during the COVID-19 pandemic: A systematic review. *Sensors*, *21*(17), 1–22. https://doi.org/10.3390/s21175787
- Charyyev, B., Mansouri, M., & Gunes, M. (2021). *Modeling the Adoption of Internet of Things in Healthcare : A Systems Approach*. *July*. https://doi.org/10.1109/ISSE51541.2021.9582493
- Chen, W., Zhu, S., Li, J., Wu, J., Chen, C. L., & Deng, Y. Y. (2021). Authorized shared electronic medical record system with proxy re-encryption and blockchain technology. *Sensors*, *21*(22). https://doi.org/10.3390/s21227765
- Chen, Z., Xu, W., Wang, B., & Yu, H. (2021). A blockchain-based preserving and sharing system for medical data privacy. *Future Generation Computer Systems*, *124*, 338–350. https://doi.org/10.1016/j.future.2021.05.023
- Churi, P., Pawar, A., Moreno-Guerrero, A.-J., Churi, P. ;, Pawar, A. ;, Moreno-Guerrero, A.-J. A., Abdul, M., & Liu, C.-H. (2021). A Comprehensive Survey on Data Utility and Privacy: Taking Indian Healthcare System as a Potential Case Study. *Inventions 2021, Vol. 6, Page 45*, *6*(3), 45. https://doi.org/10.3390/INVENTIONS6030045
- *Code of Medical Ethics Regulations, 2002 | NMC*. (n.d.). Retrieved September 21, 2022, from https://www.nmc.org.in/rules-regulations/code-

of-medical-ethics-regulations-2002/

- Coleman, J. B. (2005). Digital Photography and the Internet, Rethinking Privacy Law. *Journal of Intellectual Property Law*, *13*. https://heinonline.org/HOL/Page?handle=hein.journals/intpl13&id=211&div=11&collection=journals
- Collins, F. S., & Varmus, H. (2015). A New Initiative on Precision Medicine. *New England Journal of Medicine*, *372*(9), 793–795. https://doi.org/10.1056/NEJMP1500523/SUPPL_FILE/NEJMP1500523_DISCLOSURES.PDF
- da Fonseca, M. H., Kovaleski, F., Picinin, C. T., Pedroso, B., & Rubbo, P. (2021). E-health practices and technologies: A systematic review from 2014 to 2019. *Healthcare (Switzerland)*, *9*(9), 1–32. https://doi.org/10.3390/healthcare9091192
- Daigle, B., & Khan, M. (2020). *United States International Trade Commission Journal of International Commerce and Economics The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities*. https://www.usitc.gov/journals.
- de Fazio, R., Giannoccaro, N. I., Carrasco, M., Velazquez, R., & Visconti, P. (2021). Wearable devices and IoT applications for symptom detection, infection tracking, and diffusion containment of the COVID-19 pandemic: a survey. *Frontiers of Information Technology and Electronic Engineering*, *22*(11), 1413–1442. https://doi.org/10.1631/FITEE.2100085
- Deep, A. (2022). Regulations for medical devices in the United States. *Medical Device Regulations*, 23–32. https://doi.org/10.1016/B978-0-323-91126-9.00009-2
- Desouza, K. C. (2005). Knowledge Management in Hospitals. *Https://Services.Igi-Global.Com/Resolvedoi/Resolve.Aspx?Doi=10.4018/978-1-59140-459-0.Ch002*, 14–28. https://doi.org/10.4018/978-1-59140-459-0.CH002
- Determann, L. (2019). Privacy and Data Protection. *Moscow Journal of International Law*, *2019*(1), 18–26. https://doi.org/10.24833/0869-0049-2019-1-18-26
- Dimitrov, D. V. (2016). Medical internet of things and big data in

healthcare. *Healthcare Informatics Research*, *22*(3), 156–163. https://doi.org/10.4258/hir.2016.22.3.156

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (1995).
- Djelouat, H., Al Disi, M., Boukhenoufa, I., Amira, A., Bensaali, F., Kotronis, C., Politi, E., Nikolaidou, M., & Dimitrakopoulos, G. (2020). Real-time ECG monitoring using compressive sensing on a heterogeneous multicore edge-device. *Undefined*, *72*. https://doi.org/10.1016/J.MICPRO.2019.06.009
- Durkin, N. (2006). Using record review as a quality improvement process. *Home Healthcare Nurse*, *24*(8), 492–504. https://doi.org/10.1097/00004045-200609000-00006
- *Eisenstadt v. Baird*. (1972). https://h2o.law.harvard.edu/cases/923
- *Electronic Health Records: Manual for Developing Countries*. (2006).
- *Electronic Medical Record Systems | Digital Healthcare Research*. (n.d.). Retrieved June 19, 2022, from https://digital.ahrq.gov/electronic-medical-record-systems#one
- Elhoseny, M., Haseeb, K., Shah, A. A., Ahmad, I., Jan, Z., & Alghamdi, M. I. (2021). Iot solution for ai-enabled privacy-preserving with big data transferring: An application for healthcare using blockchain. *Energies*, *14*(17). https://doi.org/10.3390/en14175364
- Elhoseny, M., Thilakarathne, N. N., Alghamdi, M. I., Mahendran, R. K., Gardezi, A. A., Weerasinghe, H., & Welhenge, A. (2021). Security and privacy issues in medical internet of things: Overview, countermeasures, challenges and future directions. *Sustainability (Switzerland)*, *13*(21). https://doi.org/10.3390/su132111645
- Elngar, A., Pawar, A., & Churi, P. (2021). *Data Protection and Privacy in Healthcare : Research and Innovations*. CRC Press. https://www.routledge.com/Data-Protection-and-Privacy-in-Healthcare-Research-and-Innovations/Elngar-Pawar-Churi/p/book/9780367501082
- ElRahman, S. A., & Alluhaidan, A. S. (2021). Blockchain technology and IoT-edge framework for sharing healthcare services. *Soft Computing*,

25(21), 13753–13777. https://doi.org/10.1007/s00500-021-06041-4

- Emerson, T. I. (1979). The Right of Privacy and Freedom of the Press. *Harvard Civil Rights-Civil Liberties Law Review* , *14*. https://heinonline.org/HOL/Page?handle=hein.journals/hcrcl14&id=337&div=17&collection=journals
- Evans, R. S. (2016). Electronic Health Records: Then, Now, and in the Future. *Yearbook of Medical Informatics*, *Suppl 1*, S48. https://doi.org/10.15265/IYS-2016-S006
- *Fair Health Information Practices Act of 1997* . (n.d.). Retrieved December 7, 2022, from https://www.govtrack.us/congress/bills/105/hr52
- Farber, H. B. (2016). Keep out: The Efficacy of Trespass, Nuisance and Privacy Torts as Applied to Drones. *Georgia State University Law Review*, *33*. https://heinonline.org/HOL/Page?handle=hein.journals/gslr33&id=393&div=26&collection=journals
- Fatoum, H., Hanna, S., Halamka, J. D., Sicker, D. C., Spangenberg, P., & Hashmi, S. K. (2021). Blockchain Integration With Digital Technology and the Future of Health Care Ecosystems: Systematic Review. *Journal of Medical Internet Research*, *23*(11), e19846. https://doi.org/10.2196/19846
- Ferrag, M. A., Shu, L., & Choo, K. K. R. (2021). Fighting COVID-19 and Future Pandemics with the Internet of Things: Security and Privacy Perspectives. *IEEE/CAA Journal of Automatica Sinica*, *8*(9), 1477–1499. https://doi.org/10.1109/JAS.2021.1004087
- *Fog Computing Employed Computer Aided Cancer Classification System Using Deep Neural Network in Internet of Things Based Healthcare System. - Abstract - Europe PMC*. (n.d.). Retrieved December 7, 2022, from https://europepmc.org/article/MED/31853735
- Fruhlinger, J. (2021, February 8). *COPPA explained: How this law protects children's privacy*.
- *Furniss v. Fitchett* . (1958). https://openlibrary.org/books/OL21450414M/Furniss_v._Fitchett
- Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, *89*(3), 421. https://doi.org/10.2307/795891

- *Govind vs State Of Madhya Pradesh & Anr* . (1975, March 18). https://indiankanoon.org/doc/436241/
- *Griswold v. Connecticut* . (1965). https://mtsu.edu/first-amendment/article/579/griswold-v-connecticut
- Guler, I., Basturk, N., Samutoglu, N., & Kucuk, K. (2018). Real-Time Abnormal Detection for Asthma Patients with Internet of Things Technology. *UBMK 2018 - 3rd International Conference on Computer Science and Engineering*, 269–274. https://doi.org/10.1109/UBMK.2018.8566452
- Gunasekeran, D. V., Tseng, R. M. W. W., Tham, Y. C., & Wong, T. Y. (2021). Applications of digital health for public health responses to COVID-19: a systematic scoping review of artificial intelligence, telehealth and related technologies. *Npj Digital Medicine*, *4*(1), 36–41. https://doi.org/10.1038/s41746-021-00412-9
- Haleem, A., & Javaid, M. (2019). Additive Manufacturing Applications in Industry 4.0: A Review. *Journal of Industrial Integration and Management*, *04*(04), 1930001. https://doi.org/10.1142/s2424862219300011
- Hamid, S. (2016). *The Opportunities and Risks of Artificial Intelligence in Medicine and Healthcare*. https://doi.org/10.17863/CAM.25624
- *Harnessing the Power of Data in Health*. (2017).
- *Harris Interactive Inc. -- Company History*. (n.d.). Retrieved December 7, 2022, from https://www.company-histories.com/Harris-Interactive-Inc-Company-History.html
- Haux, R. (2006). Health information systems - Past, present, future. *International Journal of Medical Informatics*, *75*(3-4 SPEC. ISS.), 268–281. https://doi.org/10.1016/J.IJMEDINF.2005.08.002
- *Health Administration Act* . (1982). https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1982-135
- *Health Insurance*. (n.d.). Retrieved October 3, 2022, from https://www.policybazaar.com/health-insurance/health-insurance-india/?msclkid=9b21f1f943c6154306ac92c3293bb495&utm_source=bing

&utm_medium=cpc&utm_term=%2Bbest %2Bmedical %2Binsurance&utm_campaign=Health_BMM_Desktop00Medical_Insurance&msclkid=9b21f1f943c6154306ac92c3293bb495

- *Healthcare in India – 2022 and beyond*. (2022, February 25). https://www.ey.com/en_in/health/healthcare-in-india-2022-and-beyond
- *Healthcare Sector Loan*. (n.d.). Retrieved October 3, 2022, from https://accessbankplc.com/business/cbn-healthcare-sector-loan
- *Healthcare Supply Chain*. (n.d.). Retrieved October 3, 2022, from https://procurementpartners.com/healthcare-supply-chain/
- Hebbale, A., Vinay, G. H. R., Krishna, B. V., & Shah, J. (2021). IoT and Machine Learning based Self Care System for Diabetes Monitoring and Prediction. *2021 2nd Global Conference for Advancement in Technology, GCAT 2021*, 1–7. https://doi.org/10.1109/GCAT52182.2021.9587681
- Hecht, J. (2018, November 30). *How Technology Is Driving Change In Almost Every Major Industry*. https://www.forbes.com/sites/jaredhecht/2018/11/30/how-technology-is-driving-change-in-almost-every-major-industry/?sh=7c0a1b342f6f
- Heshmat, M., & Shehata, A.-R. S. (n.d.). *A Framework about Using Internet of Things for Smart Cancer Treatment Process*.
- Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R., & Taylor, R. (2005). Can electronic medical record systems transform health care? Potential health benefits, savings, and costs. *Health Affairs (Project Hope)*, *24*(5), 1103–1117. https://doi.org/10.1377/HLTHAFF.24.5.1103
- *HIPAA and Your Privacy Rights*. (1996). Cdph. https://www.cdph.ca.gov/Programs/OLS/Pages/HIPAA-and-Your-Privacy-Rights.aspx
- *History of Privacy Timeline*. (1980). Safe Computing. https://safecomputing.umich.edu/privacy/history-of-privacy-timeline
- Holvast, J. (2008). History of Privacy. *Undefined*, *298*, 13–42. https://doi.org/10.1007/978-3-642-03315-5_2
- Hoover, R. (2017). Benefits of using an electronic health record. *Nursing Critical Care*, *12*(1), 9–10.

https://doi.org/10.1097/01.CCN.0000508631.93151.8D

- *Hospital*. (2022). https://www.who.int/health-topics/hospitals#tab=tab_1
- Hossain, M. A., Hossain, M. E., & Rahaman, M. A. (2021). Multipurpose medical assistant robot (Docto-Bot) based on internet of things. *International Journal of Electrical and Computer Engineering*, *11*(6), 5558–5567. https://doi.org/10.11591/ijece.v11i6.pp5558-5567
- *How AI and machine learning are helping to tackle COVID-19 | World Economic Forum*. (2022). https://www.weforum.org/agenda/2020/05/how-ai-and-machine-learning-are-helping-to-fight-covid-19/
- *How can electronic lab results help me improve patient care?* (n.d.). HealthIT.Gov. Retrieved February 5, 2024, from https://www.healthit.gov/faq/how-can-electronic-lab-results-help-me-improve-patient-care
- *Human rights*. (n.d.). Who. Retrieved February 5, 2024, from https://www.who.int/health-topics/human-rights#tab=tab_1
- *IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years*. (2019, July 23). IBM. https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years
- Ilyas, T., Mahmood, D., Ahmed, G., & Akhunzada, A. (2021). Symptom analysis using fuzzy logic for detection and monitoring of covid-19 patients. *Energies*, *14*(21). https://doi.org/10.3390/en14217023
- *Importance Of Diagnostic Centre – PDC Health*. (n.d.). Retrieved October 3, 2022, from https://pdchealth.wordpress.com/2017/12/04/importance-of-diagnostic-centre/
- Imran, M., Zaman, U., Imran, Imtiaz, J., Fayaz, M., & Gwak, J. (2021). Comprehensive survey of iot, machine learning, and blockchain for health care applications: A topical assessment for pandemic preparedness, challenges, and solutions. *Electronics (Switzerland)*, *10*(20), 1–37. https://doi.org/10.3390/electronics10202501
- *India--diabetes capital of the world: now heading towards hypertension*. (2007). PubMed. https://pubmed.ncbi.nlm.nih.gov/17844690/

- *India Overtaking China as the World's Most Populous Country* . (2023, April). https://webtv.un.org/en/asset/k14/k14c0ov9sb
- *India Population* . (2023). Worldometer. https://www.worldometers.info/world-population/india-population/
- *Indian Healthcare Industry Analysis | IBEF*. (2022). https://www.ibef.org/industry/healthcare-presentation
- *Information Bureau*. (n.d.). Pib.Gov. Retrieved February 5, 2024, from https://pib.gov.in/indexd.aspx
- Ingalls, S. (2021). *The IoT Cybersecurity Act of 2020: Implications for Devices*.
- *International Covenant on Economic, Social and Cultural Rights | OHCHR*. (1966). https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights
- Ioannidou, I., & Sklavos, N. (2021). On general data protection regulation vulnerabilities and privacy issues, for wearable devices and fitness tracking applications. *Cryptography*, *5*(4). https://doi.org/10.3390/cryptography5040029
- Iranpak, S., Shahbahrami, A., & Shakeri, H. (2021). Remote patient monitoring and classifying using the internet of things platform combined with cloud computing. *Journal of Big Data*, *8*(1). https://doi.org/10.1186/s40537-021-00507-w
- Ishtiaque, F., Sadid, S. R., Kabir, M. S., Ahalam, S. O., & Wadud, M. S. I. (2021). IoT-Based Low-cost Remote Patient Monitoring and Management system with Deep Learning-Based Arrhythmia and Pneumonia detection. *2021 IEEE 4th International Conference on Computing, Power and Communication Technologies, GUCON 2021*, 1–6. https://doi.org/10.1109/GUCON50781.2021.9573620
- *IT Act & SPDI Rules: Data Protection Regime of India*. (2021). Tssaro. https://tsaaro.com/blogs/it-act-spdi-rules-data-protection-regime-of-india/
- Jaigirdar, F. T., Rudolph, C., & Bain, C. (2021). Risk and Compliance in IoT- Health Data Propagation: A Security-Aware Provenance based

Approach. *Proceedings - 2021 IEEE International Conference on Digital Health, ICDH 2021*, *September*, 27–37. https://doi.org/10.1109/ICDH52753.2021.00015

- Jan, M. A., Khan, F., Mastorakis, S., Adil, M., Akbar, A., & Stergiou, N. (2021). LightIoT: Lightweight and secure communication for energy-efficient IoT in health informatics. *IEEE Transactions on Green Communications and Networking*, *5*(3), 1202–1211. https://doi.org/10.1109/TGCN.2021.3077318
- Jara, A. J., Belchi, F. J., Alcolea, A. F., Santa, J., Zamora-Izquierdo, M. A., & Gómez-Skarmeta, A. F. (2010). A pharmaceutical intelligent information system to detect allergies and adverse drugs reactions based on internet of things. *2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM Workshops 2010*, 809–812. https://doi.org/10.1109/PERCOMW.2010.5470547
- Jiang, F., Jiang, Y., Zhi, H., Dong, Y., Li, H., Ma, S., Wang, Y., Dong, Q., Shen, H., & Wang, Y. (2017a). Artificial intelligence in healthcare: Past, present and future. *Stroke and Vascular Neurology*, *2*(4), 230–243. https://doi.org/10.1136/svn-2017-000101
- Jiang, F., Jiang, Y., Zhi, H., Dong, Y., Li, H., Ma, S., Wang, Y., Dong, Q., Shen, H., & Wang, Y. (2017b). Artificial intelligence in healthcare: past, present and future. *Stroke and Vascular Neurology*, *2*(4), 230–243. https://doi.org/10.1136/SVN-2017-000101
- Jr., B. M. (1984). *Privacy Studies in Social and Cultural History*.
- *Justice K.S.Puttaswamy(Retd) vs Union Of India*. (2017). Indian Kanoon. https://indiankanoon.org/doc/127517806/
- Kalita, J., & Emilia, V. (2018). *Advances in Intelligent Systems and Computing 740 Recent Developments in Machine Learning and Data Analytics*.
- Keehan, S. P., Cuckler, G. A., Poisal, J. A., Sisko, A. M., Smith, S. D., Madison, A. J., Rennie, K. E., Fiore, J. A., & Hardesty, J. C. (2020). National Health Expenditure Projections, 2019-28: Expected Rebound In Prices Drives Rising Spending Growth. *Health Affairs (Project Hope)*, *39*(4), 704–714. https://doi.org/10.1377/HLTHAFF.2020.00094

- *Kharak Singh vs The State Of U. P. & Others* . (1962, December 18). https://indiankanoon.org/doc/619152/
- Knickerbocker, J. U., Budd, R., Dang, B., Chen, Q., Colgan, E., Hung, L. W., Kumar, S., Lee, K. W., Lu, M., Nah, J. W., Narayanan, R., Sakuma, K., Siu, V., & Wen, B. (2018). *Heterogeneous Integration Technology Demonstrations For Future Healthcare , IoT , and AI Computing Solutions*. 1519–1528. https://doi.org/10.1109/ECTC.2018.00231
- Kuner, C., Cate, F. H., Millard, C., & Svantesson, D. J. B. (2013). The extraterritoriality of data privacy laws-an explosive issue yet to detonate. *International Data Privacy Law*, *3*(3), 147–148. https://doi.org/10.1093/idpl/ipt009
- Lau, F., Price, M., Boyd, J., Partridge, C., Bell, H., & Raworth, R. (2012). Impact of electronic medical record on physician practice in office settings: A systematic review. *BMC Medical Informatics and Decision Making*, *12*(1), 1–10. https://doi.org/10.1186/1472-6947-12-10/FIGURES/3
- Le, D. N., Van Le, C., Tromp, J. G., & Nguyen, G. N. (2018). Emerging technologies for health and medicine virtual reality, augmented reality, Artificial intelligence, internet of Things, robotics, industry 4.0. In *Emerging Technologies for Health and Medicine: Virtual Reality, Augmented Reality, Artificial Intelligence, Internet of Things, Robotics, Industry 4.0*. wiley. https://doi.org/10.1002/9781119509875
- Lederman, R., Ben-assuli, O., & Hong, T. (2021). The role of the Internet of Things in Healthcare in supporting clinicians and patients : A narrative review. *Health Policy and Technology*, *10*(3), 100552. https://doi.org/10.1016/j.hlpt.2021.100552
- Lederman, R., Ben-Assuli, O., & Vo, T. H. (2021). The role of the Internet of Things in Healthcare in supporting clinicians and patients: A narrative review. *Health Policy and Technology*, *10*(3), 100552. https://doi.org/10.1016/j.hlpt.2021.100552
- Lee, I. (2017). Big data: Dimensions, evolution, impacts, and challenges. *Business Horizons*, *60*(3), 293–303. https://doi.org/10.1016/J.BUSHOR.2017.01.004
- Lee, S. (2015). LORD DENNING, MAGNA CARTA AND

MAGNANIMITY. *The Denning Law Journal*, *27*, 106–129. https://doi.org/10.5750/DLJ.V27I0.1127

- Levin, A., & Nicholson, M. J. (2005). Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground. *Undefined*.
- Li, L., Peng, H., Kurths, J., Yang, Y., & Schellnhuber, H. J. (2014). Chaos-order transition in foraging behavior of ants. *Proceedings of the National Academy of Sciences of the United States of America*, *111*(23), 8392–8397. https://doi.org/10.1073/PNAS.1407083111
- Lim, S. L., Chung, K., Ong, B., Chan, Y. H., Loke, W. C., Ferguson, M., & Daniels, L. (2012). Malnutrition and its impact on cost of hospitalization, length of stay, readmission and 3-year mortality q. *Clinical Nutrition*, *31*, 345–350. https://doi.org/10.1016/j.clnu.2011.11.001
- Liu, S. (2016). How the user liaison's understanding of development processes moderates the effects of user-related and project management risks on IT project performance. *Undefined*, *53*(1), 122–134. https://doi.org/10.1016/J.IM.2015.09.004
- M.P. Sharma & Ors. vs. Satish Chandra and Ors., (1954). https://privacylibrary.ccgnlud.org/case/saroj-rani-vs-sudarshan-kumar-chadha
- *Mail | The First Amendment Encyclopedia*. (n.d.). Retrieved September 7, 2022, from https://mtsu.edu/first-amendment/article/1130/mail
- Malarvizhi Kumar, P., Hong, C. S., Chandra Babu, G., Selvaraj, J., & Gandhi, U. D. (2021). Cloud- and IoT-based deep learning technique-incorporated secured health monitoring system for dead diseases. *Soft Computing*, *25*(18), 12159–12174. https://doi.org/10.1007/s00500-021-05866-3
- Mamdouh, M., Awad, A. I., Khalaf, A. A. M., & Hamed, H. F. A. (2021). Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions. *Computers and Security*, *111*, 102491. https://doi.org/10.1016/j.cose.2021.102491
- Mandke, S., Kudave, K., Labde, R., & Bakal, P. J. W. (2018). *IOT based Infant Health Monitoring System*. 3418–3421.
- Manogaran, G., Alazab, M., Song, H., & Kumar, N. (2021). CDP-UA:

Cognitive Data Processing Method Wearable Sensor Data Uncertainty Analysis in the Internet of Things Assisted Smart Medical Healthcare Systems. *IEEE Journal of Biomedical and Health Informatics*, *25*(10), 3691–3699. https://doi.org/10.1109/JBHI.2021.3051288

- Manyika, J., Chui Brown, M., B. J., B., Dobbs, R., Roxburgh, C., & Hung Byers, A. (2011). Big data: The next frontier for innovation, competition and productivity. *McKinsey Global Institute*, *June*, 156. https://bigdatawg.nist.gov/pdf/MGI_big_data_full_report.pdf
- Marques, G., Pires, I. M., Miranda, N., & Pitarma, R. (2019). Air Quality Monitoring Using Assistive Robots for Ambient Assisted Living and Enhanced Living Environments through Internet of Things. *Undefined*, *8*(12). https://doi.org/10.3390/ELECTRONICS8121375
- Marques, J. A. L., Han, T., Wu, W., Do Vale Madeiro, J. P., Neto, A. V. L., Gravina, R., Fortino, G., & De Albuquerque, V. H. C. (2021). IoT-Based Smart Health System for Ambulatory Maternal and Fetal Monitoring. *IEEE Internet of Things Journal*, *8*(23), 16814–16824. https://doi.org/10.1109/JIOT.2020.3037759
- Masud, M., Gaba, G. S., Alqahtani, S., Muhammad, G., Gupta, B. B., Kumar, P., & Ghoneim, A. (2021). A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care. *IEEE Internet of Things Journal*, *8*(21), 15694–15703. https://doi.org/10.1109/JIOT.2020.3047662
- *Maurya dynasty (321-184 BC)*. (n.d.). Retrieved September 7, 2022, from https://www.globalsecurity.org/military/world/india/history-mauryan.htm
- *Meaningful Use and the Shift to the Merit-based Incentive Payment System*. (n.d.). 2013. Retrieved February 6, 2024, from https://www.healthit.gov/topic/meaningful-use-and-macra/meaningful-use
- *Medical errors in top 10 killers: WHO | India News - Times of India*. (n.d.). Retrieved December 7, 2022, from https://timesofindia.indiatimes.com/india/Medical-errors-in-top-10-killers-WHO/articleshow/8032059.cms
- *Medical record management : Huffman, Edna K., 1896- : Free Download, Borrow, and Streaming : Internet Archive*. (n.d.). Retrieved December 7,

2022, from https://archive.org/details/medicalrecordmane6huff

- Mehta, N., Pandit, A., & Shukla, S. (2019). Transforming healthcare with big data analytics and artificial intelligence: A systematic mapping study. *Journal of Biomedical Informatics*, *100*. https://doi.org/10.1016/J.JBI.2019.103311
- Meng, W., Cai, Y., Yang, L. T., & Chiu, W. Y. (2021). Hybrid Emotion-Aware Monitoring System Based on Brainwaves for Internet of Medical Things. *IEEE Internet of Things Journal*, *8*(21), 16014–16022. https://doi.org/10.1109/JIOT.2021.3079461
- Meskó, B., Drobni, Z., Bényei, É., Gergely, B., & Győrffy, Z. (2017). Digital health is a cultural transformation of traditional healthcare. *MHealth*, *3*, 38–38. https://doi.org/10.21037/MHEALTH.2017.08.07
- *Millions of Highly Sensitive Patient Records Exposed in Medical Diagnostic Company Data Breach*. (2024, February 13). https://www.websiteplanet.com/news/redcliffe-breach-report/
- Minhas, A. (2023). *India: healthcare sector size 2022*. Statista. https://www-statista-com.eu1.proxy.openathens.net/statistics/701556/healthcare-sector-size-india/
- Ministry of Health and Family Welfare. (2017, July 28). *Electronic Health Record*. Press Information Bureau .
- Mohammad Hossein, K., Esmaeili, M. E., Dargahi, T., Khonsari, A., & Conti, M. (2021). BCHealth: A Novel Blockchain-based Privacy-Preserving Architecture for IoT Healthcare Applications. *Computer Communications*, *180*(December 2020), 31–47. https://doi.org/10.1016/j.comcom.2021.08.011
- Mohanta, B. (2019). *Healthcare 5.0: A paradigm shift in digital healthcare system using Artificial Intelligence, IOT and 5G Communication*. 191–196. https://doi.org/10.1109/ICAML48257.2019.00044
- Mohsin, F., & Elmedany, W. (2021). A Secure Internet of Healthcare Things for tackling COVID-19. *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies, 3ICT 2021*, 98–104. https://doi.org/10.1109/3ICT53449.2021.9581819

- Moore, A. (2008). Defining Privacy. *Journal of Social Philosophy*, *39*(3), 411–428. https://doi.org/10.1111/J.1467-9833.2008.00433.X
- Moores, T. T. (2012). Towards an integrated model of IT acceptance in healthcare. *Decision Support Systems*, *53*(3), 507–516. https://doi.org/10.1016/J.DSS.2012.04.014
- Morris, L. (2020, January 7). *The Disadvantages of Paper Medical Records*. https://www.softwareadvice.com/resources/pros-cons-paper-charts/
- *Mr. X vs. Hospital Z*. (1998). https://privacylibrary.ccgnlud.org/case/mr-x-vs-hospital-z
- Nakhla, Z., Nouira, K., & Ferchichi, A. (2019). Prescription Adverse Drug Events System (PrescADE) Based on Ontology and Internet of Things. *The Computer Journal*, *62*(6), 801–805. https://doi.org/10.1093/COMJNL/BXY076
- Nasser, A. R., Hasan, A. M., Humaidi, A. J., Alkhayyat, A., Alzubaidi, L., Fadhel, M. A., Santamaría, J., & Duan, Y. (2021). Iot and cloud computing in health-care: A new wearable device and cloud-based deep learning algorithm for monitoring of diabetes. *Electronics (Switzerland)*, *10*(21). https://doi.org/10.3390/electronics10212719
- Nations, U. (2002). National Human Development Report 2001. *Human Development Reports*.
- Nguyen Gia, T., Dhaou, I. Ben, Ali, M., Rahmani, A. M., Westerlund, T., Liljeberg, P., & Tenhunen, H. (2019). Energy efficient fog-assisted IoT system for monitoring diabetic patients with cardiovascular disease. *Future Generation Computer Systems*, *93*, 198–211. https://doi.org/10.1016/J.FUTURE.2018.10.029
- Nigar, N., & Chowdhury, L. (2018). An Intelligent Children Healthcare System by Using Ensemble Technique. *Undefined*, 137–150. https://doi.org/10.1007/978-981-13-7564-4_12
- Nikooghadam, M., Amintoosi, H., & Kumari, S. (2021). On the Security of "Secure and Lightweight Authentication with Key Agreement for Smart Wearable Systems." *Wireless Personal Communications*, *120*(1). https://doi.org/10.1007/s11277-021-08430-2

- Nikooghadam, M., Amintoosi, H., Kumari, S., Jan, M. A., Khan, F., Mastorakis, S., Adil, M., Akbar, A., Stergiou, N., Malarvizhi Kumar, P., Hong, C. S., Chandra Babu, G., Selvaraj, J., Gandhi, U. D., Pathak, N., Deb, P. K., Mukherjee, A., Misra, S., Saba, T., … Tanwar, S. (2021). Digital Twin for Intelligent Context-Aware IoT Healthcare Systems. *IEEE Internet of Things Journal*, *8*(21), 1–22. https://doi.org/10.1109/JIOT.2020.3033129
- Nimbalkar, N. (2011). John Locke on Privacy . *Mens Sana Monographs*, *9*(1), 268. https://doi.org/10.4103/0973-1229.77443
- Novak, D., & Riener, R. (2015). Control Strategies and Artificial Intelligence in Rehabilitation Robotics. *Undefined*, *36*(4), 23–33. https://doi.org/10.1609/AIMAG.V36I4.2614
- Office of Civil Rights, H. (2013). *HIPAA Administrative Simplification Regulation Text*.
- Oladele, D. A., Markus, E. D., & Abu-Mahfouz, A. M. (2021). Adaptability of assistive mobility devices and the role of the internet of medical things: Comprehensive review. *JMIR Rehabilitation and Assistive Technologies*, *8*(4). https://doi.org/10.2196/29610
- *Olmstead v. United States*. (1928). https://constitutioncenter.org/the-constitution/supreme-court-case-library/olmstead-v-united-states
- *Ornstein, S.M., Oates, R.B. and Fox, G.N. (1992) The Computer-Based Medical Record Current Status. Journal of Family Practice, 35, 556-565. - References - Scientific Research Publishing*. (1992). https://www.scirp.org/(S(i43dyn45teexjx455qlt3d2q))/reference/referencespapers.aspx?referenceid=1495977
- Orwell, G. (1984). *1984* . https://bookanalysis.com/george-orwell/1984/
- Ota, H., Chao, M., Gao, Y., Wu, E., Tai, L. C., Chen, K., Matsuoka, Y., Iwai, K., Fahad, H. M., Gao, W., Nyein, H. Y. Y., Lin, L., & Javey, A. (2017). 3D printed “earable” smart devices for real-time detection of core body temperature. *ACS Sensors*, *2*(7), 990–997. https://doi.org/10.1021/ACSSENSORS.7B00247
- *Overview: Children’s Online Privacy Protection Act (COPPA)*. (2021, November). https://usercentrics.com/knowledge-hub/childrens-online-protection-act-coppa/

- Panch, T., Szolovits, P., & Atun, R. (2018). Artificial intelligence, machine learning and health systems. *Journal of Global Health*, *8*(2). https://doi.org/10.7189/JOGH.08.020303
- Pantelopoulos, A., & Bourbakis, N. G. (2010). A survey on wearable sensor-based systems for health monitoring and prognosis. *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews*, *40*(1), 1–12. https://doi.org/10.1109/TSMCC.2009.2032660
- Panunzio, N., Bianco, G. M., Occhiuzzi, C., & Marrocco, G. (2021). RFID sensors for the monitoring of body temperature and respiratory function: A pandemic prospect. *2021 6th International Conference on Smart and Sustainable Technologies, SpliTech 2021*, *d*. https://doi.org/10.23919/SpliTech52315.2021.9566334
- Pathak, N., Deb, P. K., Mukherjee, A., & Misra, S. (2021). IoT-to-the-Rescue: A Survey of IoT Solutions for COVID-19-Like Pandemics. *IEEE Internet of Things Journal*, *8*(17), 13145–13164. https://doi.org/10.1109/JIOT.2021.3082838
- Pathak, N., Misra, S., Mukherjee, A., & Kumar, N. (2021). HeDI: Healthcare Device Interoperability for IoT-Based e-Health Platforms. *IEEE Internet of Things Journal*, *8*(23), 16845–16852. https://doi.org/10.1109/JIOT.2021.3052066
- Paul, S., Riffat, M., Yasir, A., Mahim, M. N., Sharnali, B. Y., Naheen, I. T., Rahman, A., & Kulkarni, A. (2021). Industry 4.0 applications for medical/healthcare services. *Journal of Sensor and Actuator Networks*, *10*(3), 1–32. https://doi.org/10.3390/jsan10030043
- *Personal Privacy in an Information Society*. (1977, July). https://archive.epic.org/privacy/ppsc1977report/
- Petrosyan, A. (2023, May 15). *Largest healthcare data breaches to date in the U.S. 2023*. Statista.
- *Pharmaceutical Company Definition | Law Insider*. (n.d.). Retrieved October 3, 2022, from https://www.lawinsider.com/dictionary/pharmaceutical-company
- *Pharmacists and the Role they Play in Healthcare | United MSD Foundation*. (n.d.). Retrieved October 3, 2022, from

https://curemsd.org/pharmacists-and-the-role-they-play-in-healthcare/

- Pirbhulal, S., Samuel, O. W., Wu, W., Sangaiah, A. K., & Li, G. (2019). A joint resource-aware and medical data security framework for wearable healthcare systems. *Future Generation Computer Systems*, *95*, 382–391. https://doi.org/10.1016/j.future.2019.01.008
- Poongodi, M., Sharma, A., Hamdi, M., Maode, M., & Chilamkurti, N. (2021). Smart healthcare in smart cities: wireless patient monitoring system using IoT. *Journal of Supercomputing*, *77*(11), 12230–12255. https://doi.org/10.1007/s11227-021-03765-w
- *Population Clock*. (n.d.). Census . Retrieved February 9, 2024, from https://www.census.gov/popclock/
- Pradeep, S., & Sharma, Y. K. (2020). Storing live sensor data to the platforms of internet of things (Iot) using arduino and associated microchips. *Advances in Intelligent Systems and Computing*, *1090*, 1–15. https://doi.org/10.1007/978-981-15-1480-7_1
- Pradhan, K., & Chawla, P. (2020). Medical Internet of things using machine learning algorithms for lung cancer detection. *Journal of Management Analytics*, *7*(4), 591–623. https://doi.org/10.1080/23270012.2020.1811789
- *PRIVACY | meaning, definition in Cambridge English Dictionary*. (n.d.). Retrieved August 27, 2022, from https://dictionary.cambridge.org/dictionary/english/privacy
- *Privacy Act*. (1974). https://www.justice.gov/opcl/privacy-act-1974
- *Privacy Definition & Meaning - Merriam-Webster*. (n.d.). Retrieved July 26, 2022, from https://www.merriam-webster.com/dictionary/privacy
- *Privatization in Health Care Services !! - Public Health Notes*. (n.d.). Retrieved October 3, 2022, from https://www.publichealthnotes.com/privatization-in-health-care-services/#Introduction
- Priya, R. L., & Vinila Jinny, S. (2021). Elderly healthcare system for chronic ailments using machine learning techniques - A review. *Iraqi Journal of Science*, *62*(9), 3138–3151. https://doi.org/10.24996/ijs.2021.62.9.29

- Prosser, W. L., & N. (1960). Privacy. *California Law Review*, *97*(2), 301–355. https://doi.org/10.4324/9781315246024-13
- *Qin dynasty of the Ancient China (221-206 BC) | Short history website*. (n.d.). Retrieved September 7, 2022, from https://www.shorthistory.org/ancient-civilizations/ancient-china/qin-dynasty-of-the-ancient-china/
- *R. Rajagopal vs State Of T.N*. (1994). https://indiankanoon.org/doc/501107/
- R joshi, S., & M Parilh, R. (n.d.). *Healthcare - Overview*. Occupational Safety and Health Administration. Retrieved February 5, 2024, from https://www.osha.gov/healthcare
- Rahman, O., Shamrat, F. M. J. M., Kashem, M. A., Akter, F., Chakraborty, S., Ahmed, M., & Mustary, S. (2022). Internet of things based electrocardiogram monitoring system using machine learning algorithm. *International Journal of Electrical and Computer Engineering*, *12*(4), 3739–3751. https://doi.org/10.11591/IJECE.V12I4.PP3739-3751
- Raji, A., Kanchana Devi, P., Golda Jeyaseeli, P., & Balaganesh, N. (2016). Respiratory monitoring system for asthma patients based on IoT. *Undefined*. https://doi.org/10.1109/GET.2016.7916737
- Randazzo, V., Ferretti, J., & Pasero, E. (2021). Anytime ecg monitoring through the use of a low-cost, user-friendly, wearable device. *Sensors*, *21*(18), 1–17. https://doi.org/10.3390/s21186036
- Reiman, J. H. (1976). *Privacy, Intimacy, and Personhood* . JSTOR. https://www.jstor.org/stable/2265060
- *Roe v. Wade*. (1973). https://www.law.cornell.edu/wex/roe_v_wade_%281973%29
- *Rule 3: Sensitive personal data or information*. (2011). https://www.itlaw.in/rule-3-sensitive-personal-data-or-information/
- Saba, T., Haseeb, K., Ahmed, I., & Rehman, A. (2020). Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. *Journal of Infection and Public Health*, *13*(10), 1567–1575. https://doi.org/10.1016/j.jiph.2020.06.027
- Sahana S Khamitkar. (2020). IoT based System for Heart Rate Monitoring.

International Journal of Engineering Research And, *V9*(07), 1563–1571. https://doi.org/10.17577/ijertv9is070673

- Sandeepa, C., Moremada, C., Dissanayaka, N., Gamage, T., & Liyanage, M. (2020). An emergency situation detection system for ambient assisted living. *2020 IEEE International Conference on Communications Workshops, ICC Workshops 2020 - Proceedings*. https://doi.org/10.1109/ICCWORKSHOPS49005.2020.9145053
- Scott, S. A. (2011). Personalizing medicine with clinical pharmacogenetics. *Genetics in Medicine*, *13*(12), 987. https://doi.org/10.1097/GIM.0B013E318238B38C
- *Section 14 in The Information Technology Act*. (2000). https://indiankanoon.org/doc/242206/
- *Section 15 in The Information Technology Act*. (2000). https://indiankanoon.org/doc/1253286/
- *Section 16. Security procedures and practices*. (2000).
- *Section 2 in The Information Technology Act*. (2000).
- Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare*, *8*(2). https://doi.org/10.3390/HEALTHCARE8020133
- Sen, S. (2020, February 5). *Global Medical Data Breach:120 Million Indian Patients' Details Available On Internet For Free*. Thelogicalindian. https://thelogicalindian.com/news/maharashtra-medical-data-leak-19603
- Shackelford, S. J. (n.d.). *The Internet of things : what everyone needs to know*. 220. Retrieved May 10, 2024, from https://books.google.com/books/about/The_Internet_of_Things.html?id=0qbaDwAAQBAJ
- Shah, S. T. U., Badshah, F., Dad, F., Amin, N., & Jan, M. A. (2019). Cloud-assisted iot-based smart respiratory monitoring system for asthma patients. *EAI/Springer Innovations in Communication and Computing*, 77–86. https://doi.org/10.1007/978-3-319-96139-2_8
- Shao, J., Cao, Z., Liang, X., & Lin, H. (2010). Proxy re-encryption with keyword search. *Information Sciences*, *180*(13), 2576–2587.

https://doi.org/10.1016/j.ins.2010.03.026

- Shen, N., Bernier, T., Sequeira, L., Strauss, J., Silver, M. P., Carter-Langford, A., & Wiljer, D. (2019). Understanding the patient privacy perspective on health information exchange: A systematic review. *International Journal of Medical Informatics*, *125*, 1–12. https://doi.org/10.1016/J.IJMEDINF.2019.01.014
- Shen, Y., Zhang, H., Fan, Y., Lee, A. P., & Xu, L. (2021). Smart Health of Ultrasound Telemedicine Based on Deeply Represented Semantic Segmentation. *IEEE Internet of Things Journal*, *8*(23), 16770–16778. https://doi.org/10.1109/JIOT.2020.3029957
- Singh, A., & Chatterjee, K. (2021). Securing smart healthcare system with edge computing. *Computers and Security*, *108*, 102353. https://doi.org/10.1016/j.cose.2021.102353
- Solove, D. J. (2016). Conceptualizing privacy. *The Individual and Privacy: Volume I*, 333–401. https://doi.org/10.1145/1929609.1929610
- Somasundaram, R., & Thirugnanam, M. (2021). Review of security challenges in healthcare internet of things. *Wireless Networks*, *27*(8), 5503–5509. https://doi.org/10.1007/s11276-020-02340-0
- Sørensen, L., Skouby, K. E., & Khajuria, S. (2022). Cybersecurity and Privacy - Bridging the Gap. *Cybersecurity and Privacy - Bridging the Gap*. https://doi.org/10.1201/9781003337812/CYBERSECURITY-PRIVACY-BRIDGING-GAP-LENE-S
- Spark and Cannon. (2016). SECRETARY'S ADVISORY COMMITTEE REPORT ON AUTOMATED PERSONAL DATA SYSTEMS. *Nuclear Fuel Cycle Royal Commission Consultation and Response Agency - Citizens' Jury*, *Code 202*, 76–134.
- *Start reading Privacy in Context | Helen Nissenbaum*. (n.d.). Retrieved July 13, 2022, from https://www-sup.stanford.edu/books/extra/?id=8862&isbn=0804772894&gvp=1
- Stauch, M., Wheat, K., & Tingle, J. (2002). *Sourcebook on medical law*. 762. https://books.google.com/books/about/Sourcebook_on_Medical_Law.html?id=35xc-rzUjxsC

- Stewart, C. (2023). *AI in healthcare market size worldwide 2030*. Statista. https://www.statista.com/statistics/1334826/ai-in-healthcare-market-size-worldwide/
- Stockdale, K. (2019). Social and Political Dimensions of Hope. *Journal of Social Philosophy*, *50*(1), 28–44. https://doi.org/10.1111/josp.12270
- Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and Privacy in the Medical Internet of Things: A Review. *Security and Communication Networks*, *2018*. https://doi.org/10.1155/2018/5978636
- Taiwo Adeleke, I. (2015). Health Information Technology in Nigeria: Stakeholders' Perspectives of Nationwide Implementations and Meaningful Use of the Emerging Technology in the Most Populous Black Nation. *American Journal of Health Research*, *3*(1), 17. https://doi.org/10.11648/J.AJHR.S.2015030101.13
- *TECHNICAL FOCUS: Laboratory detection*. (2020).
- *Technology is Changing How Doctors Diagnose, Treat Patients*. (n.d.). Retrieved June 19, 2022, from https://www.govtech.com/health/technology-is-changing-how-doctors-diagnose-treat-patients.html
- *The Disadvantages of Paper Medical Records*. (n.d.). Retrieved December 8, 2022, from https://www.softwareadvice.com/resources/pros-cons-paper-charts/
- *The Indian Medical Council (Amendment) Ordinance*. (2016). Prsindia . https://prsindia.org/billtrack/the-indian-medical-council-amendment-ordinance-2016
- *The Medical Devices Rules*. (2017). https://cdsco.gov.in/opencms/opencms/system/modules/CDSCO.WEB/elements/download_file_division.jsp?num_id=OTg4NQ==
- *The Private Sector | Health Systems Global*. (n.d.). Retrieved December 7, 2022, from https://healthsystemsglobal.org/thematic-groups/the-private-sector/
- *Theorists: Philippe Ariès*. (n.d.). Retrieved July 27, 2022, from https://www.representingchildhood.pitt.edu/aries.htm

- Thilakarathne, N. N. (2020). *Security and Privacy Issues in IoT Environment*. *1*(1), 26–29.
- Thilakarathne, N. N., Kagita, M. K., & Gadekallu, D. T. R. (2020). The Role of the Internet of Things in Health Care: A Systematic and Comprehensive Study. *International Journal of Engineering and Management Research*, *10*(4), 145–159. https://doi.org/10.31033/ijemr.10.4.22
- Thompson, C. D. (2013). Benefits and Risks of Electronic Medical Record (EMR): An Interpretive Analysis of Healthcare Consumers' Perceptions of an Evolving Health Information Systems Technology. *ProQuest LLC*.
- Tierney, M. J., Pageler, N. M., Kahana, M., Pantaleoni, J. L., & Longhurst, C. A. (2013). Medical education in the electronic medical record (EMR) era: benefits, challenges, and future directions. *Academic Medicine : Journal of the Association of American Medical Colleges*, *88*(6), 748–752. https://doi.org/10.1097/ACM.0B013E3182905CEB
- Topol, E. J., Steinhubl, S. R., & Torkamani, A. (2015). Digital medical tools and sensors. *JAMA*, *313*(4), 353–354. https://doi.org/10.1001/JAMA.2014.17125
- Tran, B. X., Vu, G. T., Ha, G. H., Vuong, Q. H., Ho, M. T., Vuong, T. T., La, V. P., Ho, M. T., Nghiem, K. C. P., Nguyen, H. L. T., Latkin, C. A., Tam, W. W. S., Cheung, N. M., Nguyen, H. K. T., Ho, C. S. H., & Ho, R. C. M. (2019). Global evolution of research in artificial intelligence in health and medicine: A bibliometric study. *Journal of Clinical Medicine*, *8*(3), 360. https://doi.org/10.3390/JCM8030360
- Trudel, M. C., Marsan, J., Paré, G., Raymond, L., Ortiz De Guinea, A., Maillet, É., & Micheneau, T. (2017). Ceiling effect in EMR system assimilation: A multiple case study in primary care family practices. *BMC Medical Informatics and Decision Making*, *17*(1). https://doi.org/10.1186/s12911-017-0445-1
- Tzanou, M. (2020). Health Data Privacy under the GDPR. In *Health Data Privacy under the GDPR*. Routledge. https://doi.org/10.4324/9780429022241/HEALTH-DATA-PRIVACY-GDPR-MARIA-TZANOU

- *Understanding the Telephone Consumer Protection Act | Insights | Greenberg Traurig LLP*. (2020). Gtlaw. https://www.gtlaw.com/en/insights/2020/4/understanding-the-telephone-consumer-protection-act
- *Universal Declaration of Human Rights*. (1948). Humanium. https://www.humanium.org/en/universal-declaration/
- *US Healthcare Industry in 2023: Analysis of the health sector, healthcare trends, & future of digital health*. (2023, January 1). Insider Intelligence .
- Viceconti, M., Hunter, P., & Hose, R. (2015). Big data, big knowledge: big data for personalized healthcare. *IEEE Journal of Biomedical and Health Informatics*, *19*(4), 1209–1215. https://doi.org/10.1109/JBHI.2015.2406883
- Vulpe, A., Crăciunescu, R., Drăgulinescu, A. M., Kyriazakos, S., Paikan, A., & Ziafati, P. (2021). Enabling security services in socially assistive robot scenarios for healthcare applications. *Sensors*, *21*(20), 1–22. https://doi.org/10.3390/s21206912
- Wadhwa, M. (2020). *Electronic Health Records in India*.
- Webb, S. (2007). The effects of repetition on vocabulary knowledge. *Applied Linguistics*, *28*(1), 46–65. https://doi.org/10.1093/APPLIN/AML048
- Weber, R. H. (2013). Internet of things e Governance quo vadis ? *Computer Law & Security Review*, *29*(4), 341–347. https://doi.org/10.1016/j.clsr.2013.05.010
- Westin, A. F. (1968). *Privacy And Freedom* (Vol. 25, Issue 1).
- *What is a Clinical Information System (CIS)?* (2021). Talking HealthTech. https://www.talkinghealthtech.com/glossary/clinical-information-system-cis
- *What is artificial intelligence and how is it used?* (2020). European Parliament. https://www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used
- *What is Health Sector* . (n.d.). Retrieved September 23, 2022, from

https://www.igi-global.com/dictionary/did-health-economics-appear-were/33377

- *What is Medical Manufacturing?* (n.d.). Retrieved October 3, 2022, from https://www.sme.org/technologies/medical-additive-manufacturing/what-is-medical-manufacturing/
- *What Is Privacy? | Privacy International*. (n.d.). Retrieved August 27, 2022, from https://www.privacyinternational.org/explainer/56/what-privacy
- *Why India's healthcare system continues to lag behind | Qrius*. (n.d.). Retrieved June 28, 2022, from https://qrius.com/indias-healthcare-lag-behind/
- *World health donors* . (n.d.). Retrieved October 3, 2022, from https://www.matherhospital.org/wellness-at-mather/donating-life-the-importance-of-organ-donation/
- World Health Organization. (2019). *The Health Sector: An Operational Definition*. 1–5.
- Xin, Q., & Wu, J. (2017). A novel wearable device for continuous, non-invasion blood pressure measurement. *Computational Biology and Chemistry*, *69*, 134–137. https://doi.org/10.1016/J.COMPBIOLCHEM.2017.04.011
- Xu, C., Gao, Z., Zhang, D., Zhang, J., Xu, L., & Li, S. (2021). Applying Cross-Modality Data Processing for Infarction Learning in Medical Internet of Things. *IEEE Internet of Things Journal*, *8*(23), 16902–16910. https://doi.org/10.1109/JIOT.2021.3068775
- yang, jenny. (2024). *Number of doctors in the U.S. by state 2024* . Statista. https://www.statista.com/statistics/186269/total-active-physicians-in-the-us/
- Yang, F., Wu, Q., Hu, X., Ye, J., Yang, Y., Rao, H., Ma, R., & Hu, B. (2021). Internet-of-Things-Enabled Data Fusion Method for Sleep Healthcare Applications. *IEEE Internet of Things Journal*, *8*(21), 15892–15905. https://doi.org/10.1109/JIOT.2021.3067905
- Yang, G., Xie, L., Mäntysalo, M., Zhou, X., Pang, Z., Xu, L. Da, Kao-Walter, S., Chen, Q., & Zheng, L. R. (2014). A Health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and

intelligent medicine box. *IEEE Transactions on Industrial Informatics*, *10*(4), 2180–2191. https://doi.org/10.1109/TII.2014.2307795

- Zhang, Y., Sun, Y., Jin, R., Lin, K., & Liu, W. (2021). High-Performance Isolation Computing Technology for Smart IoT Healthcare in Cloud Environments. *IEEE Internet of Things Journal*, *8*(23), 16872–16879. https://doi.org/10.1109/JIOT.2021.3051742
- Zhao, L., Zhang, F., Ding, X., Wu, G., Lam, Y. Y., Wang, X., Fu, H., Xue, X., Lu, C., Ma, J., Yu, L., Xu, C., Ren, Z., Xu, Y., Xu, S., Shen, H., Zhu, X., Shi, Y., Shen, Q., … Zhang, C. (2018). Gut bacteria selectively promoted by dietary fibers alleviate type 2 diabetes. *Science (New York, N.Y.)*, *359*(6380), 1151–1156. https://doi.org/10.1126/SCIENCE.AAO5774
- Zhao, W., Wang, C., & Nakahira, Y. (2012). Medical application on internet of things. *IET Conference Publications*, *2011*(586 CP), 660–665. https://doi.org/10.1049/cp.2011.0751

List of Publication:

1. Kumar, Rajesh & Chopra, RK. (2023). Issues And Challenges in The Healthcare Sector Pre- Post Technological Advancement: A Review Study Using. *Asian and Pacific Economic Review.*
2. Kumar, Rajesh, Gupta, Kanchal & Chopra, RK. (2024). Medical Device Regulations: A Comparative Study, *European Economics Letters*. https://www.eelet.org.uk/index.php/journal/article/view/1029

Privacy and Protection of Patient Sensitive Data in the Healthcare Sector: A Critical Analysis

ORIGINALITY REPORT

10%	8%	5%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.nyulawglobal.org Internet Source	1%
2	digitalcommons.du.edu Internet Source	<1%
3	nluwebsite.s3.ap-south-1.amazonaws.com Internet Source	<1%
4	reproductiverights.org Internet Source	<1%
5	dr.ddn.upes.ac.in:8080 Internet Source	<1%
6	blog.ipleaders.in Internet Source	<1%
7	nhiso.com Internet Source	<1%
8	baadalsg.inflibnet.ac.in Internet Source	<1%
9	ebin.pub Internet Source	<1%