THE NATIONAL UNIVERSITY OF ADVANCED LEGAL STUDIES, KOCHI

DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTERS OF LAWS (2020-21) ON THE TOPIC

LEGAL REGULATIONS OF ELECTRONIC HEALTH RECORDS: A COMPARATIVE PERSPECTIVE

Under the guidance and supervision of
Dr. Liji Samuel

Submitted by:-
ASLAM AHAMMED S R
Register No: LM0320004
LL.M (PUBLIC HEALTH LAW)

CERTIFICATE

This is to certify that **ASLAM AHAMMED S R**, Reg. No: **LM0320004** has submitted his dissertation titled, "LEGAL REGULATIONS OF ELECTRONIC HEALTH RECORDS - COMPARATIVE PERSPECTIVE", in partial fulfilment of the requirement for the award of Degree of Master of Laws in Public Health Law to the National University of Advanced Legal Studies, Kochi under my guidance and supervision. It is also affirmed that, the dissertation submitted by him is original, bona-fide and genuine.

Date: 10-10-2021

Place: Ernakulam

Dr. Liji Samuel (Guide and Supervisor NUALS)

DECLARATION

I declare that this dissertation titled, "LEGAL REGULATIONS OF ELECTRONIC HEALTH RECORDS : A COMPARATIVE PERSPECTIVE", researched and submitted by me to the National University of Advanced Legal Studies in partial fulfilment of the requirement for the award of Degree of Master of Laws in Public Health Law, under the guidance and supervision of Dr.Liji Samuel is an original, bona-fide and legitimate work and it has been pursued for an academic interest. This work or any type thereof has not been submitted by me or anyone else for the award of another degree of either this University or any other University.

Date: 11-10-2020

Place: Ernakulam

Aslam Ahammed S R

Reg. no: LM0119022 LL.M (Public Health Law)

NUALS

ACKNOWLEDGEMENT

It is my great pleasure to acknowledge my deepest thanks and gratitude to Dr.Liji Samuel, for her valuable guidance and suggestions throughout my research. It was a great honour to work under her supervision.

I would like to extend my gratitude to the Vice-Chancellor Prof. (Dr.) K.C Sunny for his constant encouragement and support. I express my sincere thanks to Prof. (Dr.) Mini S, Director of Centre for Post Graduate Legal Studies for her supports and encouragement extended during the course.

I would further extend my deep felt gratitude to all the faculties of NUALS for their constant encouragement.

I would also like to thank the Library staff for the support rendered in collecting and compiling material for this research.

This dissertation was completed during the COVID 19 pandemic crisis when the whole world is battling and like everyone, I must express my very profound gratitude to my dear friends and batch-mates for their constant support and encouragement during the troubling times.

With genuine humility, I am thankful to The Almighty for all his uncountable bounties and blessings.

ASLAM AHAMMED S R

TABLE OF ABBREVIATIONS

1. CCHIT: Certification Commission for Health Information Technology
2. CHI: Consolidated Health Information
3. CHIE: Chief Health Information Executive
4. DHHS: Department of Health and Human Services
5. DISHA: Digital Information Security in Healthcare Act, 2018
6. DIT: Department of Information Technology
7. ECtHR: European Court of Human Rights
8. EHR: Electronic health records
9. EMR: Electronic medical records
10. GDP: Gross Domestic Product
11. GoI: Government of India
12. HDM: Health Data Management Policy, 2020
13. HHS: Health and Human Services
14. HIPAA: Health Insurance Portability and Accountability Act
15. HIS: Health Information Systems
16. HITEC: Health Information Technology for Economic and Clinical Health Act of 2009
17. HIU: Health Information User (HIU)
18. IDSP: The Integrated Disease Surveillance Programme
19. IOM: Institute of Medicine
20. MCI: Medical Council of India
21. MeitY: Ministry of Electronics and Information Technology (MeitY)
22. MoHFW: Ministry of Health and Family Welfare
23. MTP: Medical Termination of Pregnancy
24. NDHB: National Digital Health Blueprint
25. NDHE: National Digital Health Eco-system
26. NDHM: National Digital Health Mission
27. NEHA: National electronic Health Authority of India
28. NGO: Non-Governmental Organisations
29. NHP: National Health Policy
30. NHS: National Health Stack
31. NIC: National Informatics Centre

32. PDP Bill: The Personal Data Protection Bill, 2019
33. PMJAY: Pradhan Mantri Jan Arogya Yojana
34. PNDT: The Pre-Natal Diagnostic Techniques
35. RMP: Registered Medical Practitioner
36. RTH: Right to Health
37. RTI Act: Right to Information Act, 2005
38. RTP: Right to Privacy
39. SDG: Sustainable Development Goal
40. SDPI Rules: Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
41. SEHA: State electronic Health Authorities
42. STQC: Standardization Testing and Quality Certification
43. WHO: World Health Organisation

TABLE OF CASES

Sl No	Case Title	Citation
1.	Deepa Sanjeev Panicker & Ors v. State of Maharashtra	*Criminal Anticipatory Bail Application No. 513 OF 2018*
2.	Durant v. Financial Services Authority	2003 E WCA Civ 1746
3.	Govind v. State of Madhya Pradesh	AIR 1975 SC 1378
4.	I v. Finland	2008 ECHR 623
5.	Justice K.S. Puttaswamy (Retd) v. Union of India	(2017) 10 SCC 1
6.	Kharak Singh v. State of Uttar Pradesh	(1964) 1 SCR 336
7.	M.P. Sharma v. Satish Chandra	1954 SCR 1077
8.	Mr `X' v. Hospital 'Z'	(1998) 8 SCC 296
9.	Mr. Surupsingh Naik v. State of Maharashtra through Additional Secretary, General Administration Deptt.	AIR 2007 Bom 126
10.	G. P. Rawat v. Ministry of Tribal Affairs	CIC/AT/A/2007/00490
11.	People's Union for Civil Liberties (PUCL) v. Union of India	(1997) 1 SCC 301
12.	Selvi v. State of Karnataka	(2010) 7 SCC 263
13.	Sharda v. Dharmpal	AIR 2003 SC 3450
14.	Unique Identification Authority of India v. CBI	(2017) 7 SCC 157
15.	Yepthomi v. Apollo Hospital Enterprises Ltd.	AIR 1999 SC 495

TABLE OF CONTENTS

1. CHAPTER 1: INTRODUCTION

Digitalization of every industry is what we are witnessing for the last few decades. We have information technology penetrating every sector, and one such industry is healthcare, where we have telemedicine, robot-assisted surgeries, self-monitoring healthcare devices, m health, e pharmacies, etc. Digital health is defined as *"a broad umbrella term encompassing eHealth, as well as emerging areas, such as the use of advanced computing sciences in 'big data, 'genomics' and artificial intelligence."* Digital health is a broad term that encompasses e-health (m health can be considered a subset to the same), telemedicine, etc. These sectors are fast evolving and are using most modern technologies like artificial intelligence, big data, and even blockchain technologies. When all these advancements are made in the healthcare sector, the question here is, are we having ample and enough laws to regulate the same? When technology is adapting at a fast pace to meet the needs of the people, we are still held with age-old laws that were formulated decades back.

Electronic health records (EHR) are patient's electronic health information generated by any healthcare setting. EHR includes various patient demographics, medications, progress notes, vital signs, past medical history, laboratory data, radiology reports, immunization history, etc. EHR can generate evidence-based health information that may help early diagnosis, quality management, and outcome reporting. In the future electronic health, records are expected to replace the medical records that are in paper form, and it may become the primary form of health record that envisages complete, accurate information and at the same time allows universal and timely access to the health information. They can even be comprehensive data that can throw light into the complete medical history, where the chances of error are significantly less. EHR can be in any form like a distributive database or in the form of mobile applications or even maybe in the form of smart cards that anyone could carry with themselves. Various nations, including India, are trying to plan and implement national-level electronic health records (EHR). However, still, there exist certain concerns as to how the data will be protected, and to what extent personal health data are safe in the hands of the government and other private entities.

In EHR Record, the patient provides information like date of birth, height, weight, residence address, contact phone/mobile number with insurance details, guardian information with address and contact number. The physician's identity provides the physician's name, address, and contact number of the consulting doctor. Health information provides the patient's health parameters like blood group, blood pressure, blood Glucose, Heart Rate, Oxygenation of

Blood, X-Ray, Blood and urine test results, etc., with the results of transactions between patients and their health care providers. Administrative information provides administrative functions such as billing. A new record is generated for every interaction; every record is added to the health record. This series of records will become a wholly modified electronic health record system.

By designing the Electronic Health Record System, it is possible to share all available information of a patient between various departments in a hospital or even within different levels of healthcare institutions like pharmacies, clinics, laboratories, etc. The EHR system also avoids unnecessary repetitions of similar investigations, and efficient decisions are possible with it. Though there are certain benefits that the citizens may avail themselves of, there are certain liability concerns like data security issues, the effectiveness of electronic communications, etc. Electronic health data is vulnerable to improper disclosure through hacking, laptop theft, inadvertent disclosure, or deliberate leaks.[1] Once electronic information is accessed by unauthorized personnel, it can be rapidly distributed to a worldwide audience through the Internet, potentially causing humiliation, ruining careers, or causing other serious harms. [2]

When it comes to India, ours is a large country with a large population, and therefore the health infrastructure also needs to be adequate. Specialized and advanced healthcare is still a privilege for rural India.It was estimated that by 2023, there would be over 650 million internet users in the country. Despite the large base of internet users, the internet penetration rate in the country stood at around 50 percent in 2020. This meant that around half of the 1.37 billion Indians had access to the Internet that year. There has been a consistent increase in internet accessibility compared to just five years ago when the internet penetration rate was around 27 percent.[3]More and more Indians are accessing the Internet on their mobile phones. This significant behavioral change is an essential factor for digital health adoption. In 2018, about 29 percent of the country's total population were mobile internet users, expected to grow to over 35 percent or approximately 500 million users by 2023. Increased availability of cheap data plans and various government initiatives under the Digital India campaign worked together to make mobile the primary internet access in the country. Notably, 4G

[1]SharonaHoffman&AndyPodgurski,InSickness,Health,andCyberspace:Protecting the Security of Electronic Private Health Information, 48 B.C. L. REV. 331, 332–34 (2007).

[2]SharonaHoffman&AndyPodgurski,InSickness,Health,andCyberspace:Protecting the Security of Electronic Private Health Information, 48 B.C. L. REV. 331, 332–34 (2007).

[3]Statista.com, Internet usage in India - statistics & facts, Published by Sandhya Keelery, Jul 7, 2020

networks were the most widely used across urban and rural India in 2019.[4]Advanced and specialized healthcare is still a privilege for rural India, which makes up about two-thirds of our population. Only 13% of the people in rural India have access to a primary health centre, 33% to a sub-centre, and 9.6% to a hospital.[5]The concept of digital health can be utilized to overcome the deficiency in public health infrastructure, provided we have an efficient regulatory framework.

Right now in India, we are only at the primitive stages of incorporating Electronic health records and at the same time trying to formulate robust data protection laws surrounding the same. The regulatory framework that is currently proposed is studied in accordance with the digital health systems of the USA, UK, and Australia. US framework has legislation as the primary mode of regulation for electronic health records. Australia provides a right-based electronic health record system, and the UK follows a hybrid model but does not have a dedicated framework for the same. And all these three countries also have a supporting data protection framework supplementing electronic health records.

India is trying to adopt a robust legal framework for regulating the EHR regime. Currently, we have the EHR standards of 2016, which are not legally enforceable. The Draft Digital Information Security in Healthcare Act, 2018 ("DISHA"), suggests the adoption of an Electronic Health Records("EHR") system with patient rights at its core. The National Digital Health Blueprint ("NDHP") document envisages a mission-mode framework. We also have Health data management Bill, which is very close to adoption. The Personal Data Protection Bill, 2019 ("PDP Bill") has some conflicting provisions with respect to DISHA on components related to healthcare. Very recently, on August 15, 2020, the Indian Prime Minister has announced the National Digital Health Mission and health ID for every Indian citizen. However, there still exist challenges to bring the dominant private health care sector under the National Digital Health Mission and thereby ensure quality and reliability of health records. Currently, we are not sure how the above regulations will be implemented in a real case scenario since there are many overlapping and conflicting ideas. We shall see in the near future how these regulations are integrated and brought to force.

[4]Statista.com, Internet usage in India - statistics & facts, Published by Sandhya Keelery, Jul 7, 2020

[5]Panagariya, Ashok. "The Challenges and innovative solutions to rural health dilemma." Annals of neurosciences vol. 21,4 (2014): 125-7. doi:10.5214/ans.0972.7531.210401

1.1 SIGNIFICANCE OF THE STUDY

In a country like India, where a vast population is not getting the proper healthcare treatment, incorporating digital health technologies can resolve this problem to a large extend. Rural India stand very back in healthcare infrastructure and healthcare accessibility. Therefore, bringing in new digital health technologies and the concept of electronic health records has a vast potential to revolutionize the healthcare sector in India. Now when it comes to patient health data, it's very unorganized or institution-specific which makes emergency medical care challenging.

The health care data protection regime in India is lagging behind and we don't have a strong and robust mechanism to protect health data. As of now we have various draft legislations that are pending before the parliament that primarily focus on data protection. We only have very few legislations like the The Pre-Natal Diagnostic Techniques (PNDT) Act, 1994, which have express provisions for patient privacy and health informational privacy. But it's the hard truth that these are not effectively enforced and still there exist unlawful health practices that are detrimental to the patients as well as the society. When it comes to regulation Electronic Health Records particularly, we currently have Electronic Health Standards, 2016 which is not legally binding. We do not have a standardised system to maintain and protect the EHR of the patients yet. These are areas where we need effective regulations that could help adoption and protection of EHRs.

The adoption of regulated electronic health records can bring stellar changes in the Indian healthcare sector. At the same time, primary importance should be given to the privacy of all citizens in India. When it comes to healthcare data, it is very significant, and any data leaks can be fatal to the nation itself. Therefore we must have a proper regulatory mechanism to check the concepts of evolving digital health technologies and electronic health records. The healthcare sector can't stand apart in this fast-paced world where every aspect of our daily livelihood is digitalized. Therefore the only feasible way is to regulate the inevitable digitalization of the healthcare sector properly.

1.2 OBJECTIVES OF THE STUDY

The objectives of the studies are as follows:

1. To determine whether India has an adequate regulatory framework for regulating Electronic Health Records.
2. To determine the scope and Advantages of Electronic Health Records.
3. To determine whether patient privacy can be guaranteed while adopting Electronic Health Record
4. To have a comparative analysis of Health data protection regime in foreign jurisdictions like USA, UK and Australia.

1.3 RESEARCH QUESTIONS

1. *Whether Electronic Health Records can successfully replace the traditional offline health records.*
2. *Whether the current health data protection regime is adequate for ensuring informational privacy in India?*
3. *Whether the Indian regulatory framework adequate for maintaining electronic health records?*
4. *Whether the patient rights are protected in the current healthcare regime in India?*
5. *Whether the concept of privacy and electronic health record co-exist together?*
6. *Whether the proposed draft health data protection legislations are in consonance with the fast paced changes in digital health technologies ?*
7. *Whether lack of proper regulations detrimentally affect Indian healthcare regimein the long run ?*

1.4 HYPOTHESIS

The Indian health care regime is very much adaptive and equipped to incorporate modern digital technologies. There is a need for effective regulation of Electronic Health Records and Healthcare Data.

1.5 RESEARCH METHODOLOGY

The research methodology used for this work is doctrinal. The researcher intends to look into various international and national regulations and articles that focus on Electronic Health Records.

1.6 LITERATURE REVIEW

1. *Analysis of Legal and Regulatory Framework in Digital Health: A Comparison of Guidelines and Approaches in The European Union and the United States*[6]- The article highlights how the healthcare system across the globe has undergone a significant change due to the intervention of digital technologies. It majorly focuses on the need to have a robust regulatory framework to facilitate the proper use of technology. It brings about a comparative analysis of the effectiveness and outcome of the regulatory framework as implemented in the European Union and the United States of America. The article concludes that a proper regulatory framework is necessary because it builds confidence and trust in people to use digital health technologies. And to implement a practical framework, privacy, security, and data protection must be given at most importance.
2. *Digital Health in India- Legal, Regulatory, and Tax Overview*[7]- The article discusses the key trends in digital health in India. It points out various examples of digital health and the legal and regulatory framework governing the same. It finds that the present regulatory framework which intends to control the digital health systems is ambiguous and unclear. Since digital health is rapidly growing day by day, there is a need to bring in solid rules and regulations to ensure practical usage. Some of the laws that have been discussed are Information and Technology Act, 2000; drugs and Cosmetics Act, 1940 and Drugs and Cosmetics Rules, 1945; the Indian Medical Council Act, 1956, Telemedicine Guidelines, 2020; the article concludes with a strong recommendation for the need to act upon the importance of privacy while dealing with digital health services.
3. *Addressing Data Privacy in Digital Health*: *Discussion on Policies, Regulations, and Technical Standards in India*[8]- The article highlights the need to address the importance of data privacy in digital health. It widely discusses security reasons and handling privacy matters in digital health care in India. It also talks about the various ways in which Electronic Health Records (EHR) have to be maintained to ensure confidentiality while dealing with the patient's details.

[6]FaraAninha Fernandes, Georgi V Chaltikyan, Analysis of Legal and Regulatory Frameworks in Digital Health: A Comparison of Guidelines and Approaches in the European Union and United States, Journal of the International Society for Telemedicine and E health (2020).

[7]Milind Antani, Darren Punnen, Shreya Shenolikar, Digital Health in India- Legal, Regulatory and Tax Overview (2020).

[8]Manisha Mantri, R. Rajamenakshi, Gaur Sunder, Addressing Data Privacy in Digital Health: Discussion on Policies, Regulations and Technical Standards in India (2019).

4. *Electronic Health Records in India*: *Legal Framework and Regulatory Issues*[9] - The article examines the evolution and framework of electronic and digital health records regulation. It talks about the different rules that have been developed globally for the proper use of health records without compromising data security, privacy, and confidentiality. The article puts forward recommendations and suggestions to the present legal framework in India. It proposes that there is a need for independent laws in India that would govern the digital health sector other than the data protection laws in India.
5. *Security and Privacy of Electronic Health Records: Concerns and Challenges*[10]- The article majorly focuses on the concerns on privacy and security of electronic health records. The author opines that the low adoption of electronic health records by health institutions is due to significant privacy concerns. And even when such electronic health records are used, it is most necessary that proper safeguards be guaranteed to the patients. The article suggests how the same can be achieved in the near future.
6. *Digital Health in India- As envisaged by the National Health Policy (2017)*[11] – The article speaks about the key takeaway of National Health Policy, 2017, which includes the following:
    - Ensure district-level electronic database of information on health system components by 2020.
    - Strengthen the health surveillance system and establish registries for diseases of public importance by 2020.
    - Establish federated integrated health information architecture, Health Information Exchanges, and National Health Information Network by 2025.

    The essential question is whether the safeguards mentioned above have been achieved or not. The article also highlights the need for a National Digital Health Authority to regulate, deploy and develop digital health systems in India.
7. *Health Care Held Ransom: Modifications to Data Breach Security & The Future of Health Care Privacy Protection*[12]- The article begins by highlighting the need to

[9]Harleen Kaur, Electronic Health Records in India: Legal Framework and Regulatory Issues, RGNUL Student Research Review, Vol. 6 (26) (2020).
[10]Ismail Keshta, Ammar Odeh, Security and Privacy of Electronic Health Records: Concerns and Challenges, Egyptian Informatics Journal (2020).
[11]SarbandhikariSuptendra Nath, Digital Health in India – As envisaged by the National Health Policy (2017), BLDE University Journal of Health Sciences, Vol. 4, 1-6 (2019).

secure patients' valuable and private information while using digital health care systems. It suggests that to ensure data protection in cases of digital health care, there are three types of safeguards that have to be met: physical, administrative, and technical safeguards. To properly implement the standards and rules, the root causes of health care security breaches must be found out. The article also brings in recommendations as to how breaches like ransomware can be tackled.

8. *mHealth and Unregulated Data: Is this Farewell to Patient Privacy*[13]- The article points out that even development of many mHealth apps, the harsh reality is that they are not subject to regulatory frameworks. The present regulations governing mHealth are narrow and only concern a minute fraction of health applications, even including those covered by HIPAA.[14] The article focuses on mHealth applications and the privacy concerns involved. Finally, it proposes the methods to ensure data protection, consumer confidence and thereby widen the application of digital healthcare technologies.
9. *Electronic Health Records and Respect for Patient Privacy*: *A Prescription for Compatibility*[15]- The article is insightful in understanding the concept of medical records and electronic health records. It discusses an overview of HIPAA and deals with cases of protecting the privacy of patients.

1.7 CHAPTERISATION

1. **INTRODUCTION**

This chapter defines the scope of the digital health system giving special emphasis on electronic health records. This chapter shall also discuss the scope and objective of the study, the hypothesis, and the research methodology to be used during the study.

2. **ELECTRONIC HEALTH RECORDS- A NEW ERA OF HEALTH DATA**

This chapter shall comprehensively describe Electronic Health Records. This chapter shall also discuss the types of EHR and its advantages compared to the traditional offline record-keeping system. The chapter also analyses the adoption of Electronic Health Records in the Indian healthcare scenario and the concerns revolving around the same.

---

[12]Ryan M. Krisby, Health Care Held Ransom: Modifications to Data Breach Security & The Future of Heath Care Privacy Protection, Health Matrix: Journal of Law-Medicine, Vol 28 (365) (2018).

[13]J. Frazee, M. Finley, JJ Rohack, mHealth and Unregulated Data: Is this Farewell to Patient Privacy, Indiana Health Law Review, 383-414 (2016).

[14]Health Insurance Portability and Accountability Act of 1996, Public Law, 104-191, 110 Stat. 1936.

[15]Lauren Bair Jacques, Electronic Health Records and Respect for Patient Privacy: A Prescription for Compatibility, Vanderbilt Journal of Entertainment and Technology Law, Vol. 13 (441) (2011).

3. **COMPARATIVE ANALYSIS OF HEALTH DATA PROTECTION LAWS IN EU, USA, AND AUSTRALIA**.

This chapter shall look into the various regulatory frameworks adopted by different countries, including the US, the European Union, and Australia for regulating electronic health records.

4. **ELECTRONIC HEALTH RECORDS AND PATIENT PRIVACY- INDIAN PERSPECTIVE**

This chapter will look into the development of India's current legal framework for Electronic health data protection. The chapter shall also analyze different steps that the Indian Government has taken, like Digital Information Security in Healthcare Act (DISHA), Personal Data Protection Bill 2019, Health data Management Policy 2020, etc. We shall also look into the concept and evolution of the right to privacy and how the Indian healthcare protection regime complies.

5. **HEALTH INFORMATION AND RIGHT TO PRIVACY IN INDIA**

We shall also look into the concept and evolution of the right to privacy and its role in the Indian healthcare protection regime. This chapter shall also discuss the relation between right to information and right to privacy when it comes to health data. It shall also look into the changing dimensions of privacy and some of the Indian healthcare privacy regulations

6. **CONCLUSION**

This chapter shall analyze the current relevance and future of Electronic Health records. It shall also suggest some measures that could be adopted for effective implementation and regulation of EHR.

2. CHAPTER 2: ELECTRONIC HEALTH RECORDS- A NEW ERA OF HEALTH DATA

2.1 INTRODUCTION

Most hospitals in India use the manual technique of record-keeping, which relies on paper and books. Manual record keeping has significant drawbacks, such as the requirement for extensive storage facilities and the difficulty in retrieving information when needed. However, it is more legally acceptable as documentary proof because tampering with records without detection is more challenging. The computerization of medical records has resulted in medical records that are nice and orderly and can be readily kept and accessed in the modern day. Nevertheless, the prospect of easy modification without discovery is a significant worry, and as a result, they may not be widely recognized as documented proof at face value. The hospital and the doctor are responsible for demonstrating that these computer records were not altered if requested during a court hearing or other legal processes. One of the most significant concerns is protecting the confidentiality of patient data because a patient who believes their medical records have been compromised might hold the doctor and the hospital liable for negligence. Depending on the technique, videotapes of the operation, electrocardiogram or pulse oximeter charts, and continuous E.C.G. or pulse oximeter charts might all be used as evidence in a court of law. The usage of electronic medical records is growing in popularity as the technology continues to develop and improve. Even though the elimination of paper records is the ultimate goal, several issues must be addressed first.

With rapid advancements in technology, 'data' became an essential aspect of day-to-day activities. The storage of an enormous amount of physical health data was a challenge, and that's when the importance of E.H.R.s was realized. And a very crucial point that needs to be acknowledged is that E.H.R.s, when compared with paper-based records, always stood on the upper side.

2.2 ADVANTAGES OF ELECTRONIC HEALTH RECORDS.

In straightforward terms, E.H.R.s are a digital collection of health-related information of a patient in an electronic form. These can be shared through the well-connected network across various health care settings situated in different parts of the globe. It consists of demographic and personal information, including age, weight, billing information, medical history, allergic history, family medical history, etc. It reduces the chance of data redundancy and directly benefits the medical practitioners, patients, and hospital management.

The considerable increase in the adoption of E.H.R.s in the health care system can be attributed to its outstanding transparency, flexibility, accessibility, and portability. The

advantage that E.H.R.s have over paper medical records is that the latter may not be legible all the time and may contribute to medical errors. Possibilities are high that poor legibility of handwritten reports may result in a medication error. Reports indicate that these errors have been reduced by 50 to 83 percent, evidently as data and information are stored online.[16] It was also opined those numerous medical errors could be prevented using integrated information technology systems. The health card of a patient contains information about the type of treatment, patient's medical history, lifestyle, prescribed medication, test results, etc. the healthcare provider, insurance companies, government agencies, other healthcare providers such as nurses, and the medical information bureau access the patient's records.[17] The E.H.R. system also eliminates Physician-patient problems that they encounter during the course of treatment. However, electronic health data is used to suggest sufficient treatment to the patient from different specialists/physicians with the E.H.R. Physicians with Electronic records speed up the treatment with the fast accessing of digital data[18]. The health information [19]in electronic health records will be used as correct information in the right hands at the right time will support patient health care to make a correct health decision

E.H.R.s are very prominent when it comes to the standardization of forms, data input, and terminology.[20] Digital technologies provide for a more accessible mode of collection and storage of data. It is not disputed that these technologies are away from challenges. The usefulness of such technological interventions outweighs the challenges and are updated now and then. If the capacity to exchange data and information between different E.H.R.s is perfect, it will benefit the coordination of health care delivery everywhere. Further, data stored in an electronic system may be used anonymously for statistical reporting in specific matters to improve public health management and resource management quality.

E.H.R.s can be understood as a great mechanism to manage labor-intensive, lengthy, and tedious paperwork more effectively and efficiently, thereby reducing the cost of storage,

[16]Abha Agrawal, *Medication Errors: Prevention Using Information Technology System* , British Journal of Clinical Pharmacology, 6th June 2009, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2723209/, accessed on 15 May 2021

[17]Patel VL, Arocha JF, Kushniruk AW. *'Patients and physicians' understanding of health and biomedical concepts: relationship to the design of EMR systems*, 35 Journal of Biomed Inform, 8-16. 2002;

[18]GeylaniKardas, E. TurhanTunali, *Design and implementation of a smart card based healthcare information system*, , 81 Journal of Elsevier, Computer Methods and Programs in BiomedicinE, 66–78, 2005

[19]Rahimi, B., Vimarlund, V., and Timpka, T., 2009. Health information system implementation: A qualitative meta-analysis. Journal of Medical Systems. DOI 10.1007/s10916-008-9198-9

[20]'Electronic Health Record Error Prevention Approach Using Ontology in Big Data', (2015), http://webpage.pace.edu/kg71231w/docs/HPCC2015-1.pdf, accessed on 18 May 2021

refiling, and transcription. It helps with accurate and enhanced management of the data related to a patient. Some of the critical benefits of E.H.R.s are as given below:[21]

- **COSTS**: While manually storing handwritten paper, records need more personnel to maintain and manage the paper files; the accessibility and daily updating of the same is also a tedious task. Even if the initial costs of setting up an HER system are high, it is always worth the value. It can reduce the workforce, physical storage space, and time invested in managing paper files.
- **STORAGE**: E.H.R.s can be stored in a properly secured cloud, resulting in more accessible access to all those who need them. Handwritten records are difficult to manage and take up a lot of physical space. As the storage of data in E.H.R.s is synchronized, updating the same also becomes easier.
- **ACCESSIBILITY**: Needless to say, the accessibility of E.H.R.s is always at a higher footing when compared to handwritten records. It allows for easy access to the healthcare professionals regarding the patient data.
- **READABILITY AND ACCURACY**: E.H.R.s are often written using standardized abbreviations, which make them more readable and accurate across the globe, which reduces the chances of confusion, as seen in the case of handwritten paper medical records.
- **SECURITY**: Security is a significant concern for both paper and E.H.R.s. Both are equally susceptible to security threats. If a facility store records electronically without proper and effective systems, they are vulnerable to access by unauthorized individuals who can misuse the information. If records are stored in paper form, the chances are that they can be lost or damaged, or stolen due to human error.

2.3 HISTORY AND FUTURE OF ELECTRONIC HEALTH RECORDS

The history of E.H.R. can be traced back to the early 1960s, with the COSTAR system developed by Barnett at the Laboratory of Computer Science at Massachusetts General Hospital[22]. In COSTAR, the patients' medical reports were first transcribed into paper and were later fed into computer systems. Later, efforts at Duke Universities and Regenstrief Institute at Indiana University paved the way to robust Electronic Health records. Later a

[21]Ruby Sahney, *Mukesh Sharma, Electronic Health Records: A General Overview, (*2018), https://www.academia.edu/37262485/Electronic_health_records_A_general_overview, accessed on 17 May 2021

[22]Barnett GO. *The application of computer-based medical-record systems in ambulatory practice*. 310 N Engl J Med. 1643-50. 1984.

computer-based electronic record was developed at Boston's Brigham and Women's Hospital, which incorporated a summary screen that showed all details of patients at a glance.

The primary issue with the development of Electronic Health Records was the lack of standards that could be used for computer technology and clinical terminology simultaneously. The American Society for Testing and Materials promulgated a standard to describe the content and structure of computer-based systems that could be used for clinical purposes[23]. But this structure is not followed nowadays in the modern-day E.H.R.'s[24]. In 1997 the Institute of Medicine prepared a report that has become the most comprehensive study and formulated a document containing attributes for E.H.R. Nowadays, the concept of E.H.R. has changed a lot, there exist different models of E.H.R. that are being followed by various entities which include server-based, network-based, or even cloud-based, systems that are developed for respective needs within the healthcare institution. These are a small chain of E.H.R.s that work within the institution or chain of institutions. But when it comes to a country like ours, it's essential to have a network infrastructure that connects all healthcare institutions.

Further, language and culture also play an essential role in implementing a uniform E.H.R. system. The majority of these systems use English as the unified language, keeping in mind the scope of interoperability and accessibility. In the long run, if plans are developed robustly that could prevent data leak at cost, there even exists a scope of Electronic Health records at the international level. But primarily, let us hope that a unified health record system gets implemented within our country without much delay to tackle the infrastructural backwardness and bravely fight against the unprecedented situations like the Covid-19 pandemic that we are facing now.

2.4 TYPES OF DIGITAL HEALTH RECORDS

Records are used in an organization to document its day-to-day activities. More and more agencies are moving towards digital records in the past decade by significantly replacing paper records. The health sector has undergone significant changes with the introduction of digital health records. Digital health records play an important role in collecting and retrieving data and information in the health sector. The objectives behind the introduction of

[23]Lowell Vizenor, Barry Smith, Werner Ceusters, *Foundation for the Electronic Health Record: An Ontological Analysis of the HL7's Reference Information Model*

[24]N. Anju Latha, B. Rama Murthy, U. Sunitha, *Electronic Health Record, International Journal of Engineering Research & Technology*, 1(10) IJERT), December- 2012

digital health records are to provide effective and efficient healthcare to the patient.[25]It has revolutionized the age-old concept of storing data and information in writing, i.e., as hard copies in papers. During the shift from manual/ paper records to electronic formats number of terms were used to describe the move. Some of them are –

Automated Health Records (A.H.R.) was traditionally referred to as a set of computer-stored images of the regular paper medical reports. The traditional medical documents are scanned and are stored in computers, C.D.s, floppy's, etc.

Computer-based patient record (C.P.R.) was first introduced during the 1990s in the U.S.A., which refers to a set of patient information identifiable by a patient identifier. C.P.R. primarily focuses on the functions like medical alerts, medication, integrated patient data, etc.

Modern digital health records can be broadly classified into three, which are Electronic Medical Records ("E.M.R.s"), Electronic Health Records("E.H.R.s"), and Personal Health Records ("PHRs").[26]

Electronic Records ("E.R.s") are either born digitally or converted from paper records using a scanner.[27] These are formal records having intrinsic value and are subject to strict information management policies. The level of protection required in cases of E.R.s is determined based on the type of business organization. The bigger the industry, the bigger the protection and privacy policies. The significant advantages of E.R.s are,

- Provides for high speed in exchange of information between the entities.
- Helps to undertake advanced researches.
- Easy storage, updating, and retrieval of data and information.
- Reduces risk in storing hard copy written documents.

E.M.R. 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,' and have the potential to provide substantial

[25]Harleen Kaur, *Electronic Health Records in India: Legal Framework and Regulatory IssuES*, 6 RGNUL Student Research Review, 26-41 (2019)

[26]*What are the differences between Electronic Medical Record, Electronic Health Record and Personal Health Records*,https://www.healthit.gov/faq/what-are-differences-between-electronic-medical-records-electronic-health-records-and-personal, accessed on 10 May 2021

[27]Chennupati K. Ramaiah, Surya Prakash Gulla, *Electronic Medical Records Management Systems: An Overview*, (2009) https://www.researchgate.net/publication/228740128_Electronic_Medical_Records_Management_Systems_An_Overview/link/54ae492f0cf2828b29fccccc/download, accessed on 15 May 2021

benefits to physicians, clinic practices, and health organizations.[28] It helps to enhance the workflow and increase the quality of patient safety and patient care.

E.H.R.s, the most commonly used digital health record, is an evolving concept of collecting electronic health information associated with the health information of individual patients. One of the critical features of the E.H.R. system is that it ensures up-to-date data and thereby eliminates the need to search for earlier paper medical records.

At times, E.M.R. and E.H.R. are often used synonymously; however, researchers have differentiated the same.

The E.M.R. acts as a data source for E.H.R. and is created by providers for specific encounters in hospitals and ambulatory environments.[29] These are exclusive terms, and in so far as the information stored in E.M.R. is concerned, it does not travel easily out of place. At times, it has to be printed and then delivered to the medical practitioners. This essentially means that E.M.R.s are more or less similar to paper records. Whereas in the case of E.H.R.s, the outflow and accessibility of information are smooth and steady. It is designed to be accessible to all people involved in patient care, including the patient themselves.[30]

As evidenced from the name, PHR is a health record wherein the health data, and all related information associated with a patient is maintained by the patient himself.[31] This means that PHRs are controlled by the patient themselves, unlike E.M.R.s and E.H.R.s, controlled by the concerned doctors and hospitals. One of the extensively recognized definitions of PHR is the one put forward by the Markle Foundation's Personal Health Working Group, Connection for Health, which states that PHR is an internet-based set of tools that allows people to access and coordinate their lifelong health information and make appropriate parts of it available to those who need it. It offers an integrated and comprehensive view of health information, including information people generate themselves, such as symptoms and medication use,

[28]'Electronic Medical Record Systems', https://digital.ahrq.gov/key-topics/electronic-medical-record-systems#one, accessed on 10 May 2021

[29]Patrick Kierkegaard, *Electronic Health Record: Wiring Europe's Healthcare*, 27 (5)Computer Law & Security Review,503-515,2011,https://www.sciencedirect.com/science/article/abs/pii/S0267364911001257?via%3Dihub, accessed on 18 May 2021

[30]Peter Garratt, Joshua Seidman, *EMR vs. HER- What is Difference*, 4th January 2011, https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference, accessed on 18 May 2021

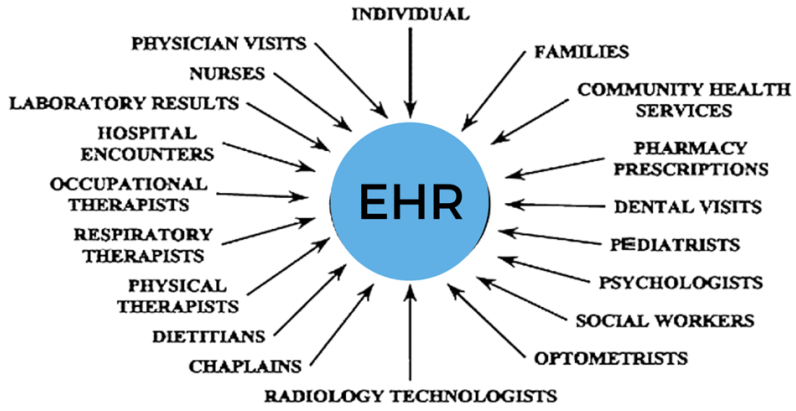
[31]Paul C. Tang, Joan S. Ash, David W. Bates, J. Marc Overhage, Daniel Z. Sands, Journal of American Medical Informatics Association, 13 April 2006, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1447551/, accessed on 18 May 2021

information from doctors such as diagnoses and test results, and information from their pharmacies and insurance companies.[32]

The World Health Organization (WHO) has proposed specific parameters in the Electronic Health Record, which states that an E.H.R. should contain all personal health information of an individual patient from his first admission at the hospital. [33]

The E.H.R. shall incorporate few ancillaries as mentioned below-

- Administrative System Components- this includes details regarding admissions,
- discharge, transfer, etc. There will also be a patient identifier that will be linked with his communication details and demographic data.
- Laboratory System Components- these Act as separate systems to integrate orders and results from the laboratory. Sometimes the machines used for testing will itself will incorporate the data with E.H.R. using machine learning technologies
- Radiology System Components- This contains information from the radiology department, comprising inferences images and other tracking functions.
- Pharmacy System Components- This includes electronic e-prescriptions automatically integrated with the pharmacy and the patient's E.H.R.
- Computerized Physician Order Entry & Clinical Documentation-This allows health service providers to order radiology, laboratory, and pharmacy services electronically.



Source: Researchgate.net (Internet)

[32]Markle Foundation, *The Personal Health Working Group*, 1st July 2003, https://web.archive.org/web/20070104212409/http://www.connectingforhealth.org/resources/final_phwg_report1.pdf, accessed 15 May 2021

[33]WHO 2006, ELECTRONIC HEALTH RECORDS: MANUAL FOR DEVELOPING COUNTRIES ,ISBN 92 9061 2177

Once all these data are collected, they are stored in healthcare databases and linked with the smart Health cards, which the patient can carry with him and show the doctor during the next consultation. Patients information's from different specific areas is combined to form the core information of the patient. To have effective functioning, E.H.R. would require the following components.

- Person Identifier
- Faculty Identifier
- Provider Identifier
- Health Information
- Administrative Information

2.5 ADOPTION OF ELECTRONIC HEALTH RECORD IN INDIAN HEALTHCARE SCENARIO

India is one of the countries where the global COVID-19 pandemic has hit very badly. We have witnessed the lack of health care infrastructure and healthcare accessibility during these bad times. The economic survey 2020-21 has suggested an increase in the country's healthcare spending from 1% to 2.5%-3.0% of the Gross Domestic Product (G.D.P.) as it's already envisaged in the National Healthcare Policy. It was noted that by doing so, the Out-of-pocket expenditure (OOPE) of healthcare could be reduced from 65% to 35% of the overall healthcare spend, thereby decreasing the burden of healthcare upon the citizens[34]. Dr. Harsh Vardhan, Union Minister of Health & Welfare, has said that "The total allocation to Health Sector in the financial year (2021-22), has increased to Rs. 2,23,846 crore from Rs. 94,452 crore the previous year (B.E. 2020-21)"[35]. India spent 1.8% of its G.D.P. in healthcare in 2021-22, which compared to the previous years were just around 1% to 1.5% of the G.D.P. Even then, it's one of the lowest spend on healthcare by any government across the world. The National Health Policy (N.H.P.)of India, which came out early in 2017, envisaged that India should spend at least 2.5 percent of its G.D.P. on the health sector by 2025.[36] But still, this remains a distant dream for us, where at the same time, some of the developed countries are spending more than 10% of their G.D.P. on healthcare. The N.H.P. 2017 shows India's

[34]Press Information Bureau, 29th Jan 2020,https://pib.gov.in/PressReleasePage.aspx?PRID=1693225, accessed on 17th May 2021
[35]Press Information Bureau, 29th Jan 2020,https://pib.gov.in/PressReleasePage.aspx?PRID=1698262, accessed on 17th May 2021
[36]National Health Portal India, 2017, https://www.nhp.gov.in/nhpfiles/national_health_policy_2017.pdf, accessed on 17th May 27, 2021.

commitment to achieving the 3rd Sustainable Development Goal (S.D.G.) of the United Nations, ensuring healthy lives and promoting well-being for all.[37]

Also, when it comes to rural India, where most people depend on government healthcare institutions, the doctor-to-patient ratio is abysmally low with 1: 10,926[38]. Apart from that, 8.57 doctors per 10,000 populations. It shows that India's doctor-patient ratio is less than the prescribed limit of 1:1000 by the WHO.[39]Amid the Covid-19 pandemic, the prime minister has announced a National Digital Health Mission, which seeks to establish a complete digital healthcare ecosystem focussing on four key features Health ID, Patient Health Records, Digi Doctor, and Health Facility, Register. Later, it also seeks to include telemedicine and e-pharmacy, for which regulatory guidelines are being framed.[40]All these seem to be a sound and broad move that could change or revolutionize the healthcare scenario, but its proper implementation and awareness is something that we should look into. In the current scenario where we lag in the number of healthcare professionals and health infrastructure, it's high time that we include the technological advancements in the healthcare system to bridge the gap between the lack of health infrastructure with the overwhelming demand for affordable healthcare. Even in the healthcare sector, digital and technological advancements have kicked in. Some examples that I would like to quote are electronic health records, lab information management systems, online health consultations, m health, Artificial intelligence in healthcare, machine learning, etc.

Technology is the right solution for some of the inadequacies that we see in our healthcare system. If we are visiting a healthcare institution or hospital, we see patients and nurses walking with a set of files. Also, when it comes to insurance penetration, we are lagging way behind when we compare with other developed countries. Concerning outpatient insurance, i.e., when we visit a doctor for our day-to-day needs, there exists no insurance coverage at all. Also, another interesting factor in India is that the patient owns the health data, unlike countries like the United States, where the healthcare data is in digital format, and nobody has access to that. The prime issue with India'shealthcare system is the complexity of the

[37]World Health Organisation. Sustainable *Development Goals, World Health Organisation (WHO),* 2020. Available online: https://www.who.int/sdg/targets/en/ (accessed on 18th, May 2020).
[38]National Health Profile, 25th June, 2019, http://www.cbhidghs.nic.in/showfile.php?lid=1147, accessed on 17th May 2021
[39]Chattu, V.K.; Yaya, *S. Emerging infectious diseases and outbreaks: Implications for women's reproductive health and rights in resource-poor settings*. 2 Reprod. Health 2020, 17.
[40]National Digital Health Mission, July 2020, https://ndhm.gov.in/, accessed on 18th May, 2021

process that a patient has to follow- let us imagine the procedure that a person with a common cold has to follow- he has to wait to get an O.P ticket, waiting for doctors, get diagnosed at a laboratory, wait for the test results, follow the same procedure for the subsequent check-up, get his medicines from the pharmacy or maybe even get admitted. By the time the person completes a single round of these procedures, the patient will have a set of documents that the majority doesn't matter to him or won't understand. Also, all these systems now remain independent of one another. The process involved and professionals involved in each stage would be unaware of what's happening in its entirety and won't be able to help the patients.

At the same time, consider the E.H.R. system where the patient just has to carry his health card, and even the attendant or receptionist at any stage would be able to help him with details regarding his health check-up. In the latter scenario, the professionals, doctors, and infrastructure remain the same. The only difference is that technology has bridged the gap by integrating various departments within the same healthcare institution.

India's digital health regulatory framework is studied and compared with that of the U.S.A., U.K., and Australia. India is in the final stages of adopting the digital healthcare framework. The collection, receipt, storage and handling, and transfer of healthcare data in electronic form come under the I.T. Data Protection Rules of 2011, a set of rules prescribed under the I.T. Act 2000 (I.T. Act 2008) and the Privacy and the Right to Information Act 2005.

India also launched voluntary Electronic health records standards in 2013[41], which was then later updated in 2016. The standards contained detailed recommendations on the interoperability and standards, clinical informatics standards, data ownership, privacy and security aspects, and the various coding systems [42]

The Draft Digital Information Security in Healthcare Act, 2018 ("DISHA") suggests an Electronic Health Record System giving primary importance to patient rights. It focuses on healthcare data privacy, confidentiality, security, and standardization of health data. The National Digital health blueprint, which is an extension of the National Health Policy 2017, aims at providing universal healthcare to all citizens using digital technologies, which further maintains higher efficiency and effectiveness. On August 15, 2020, our Hon'ble Prime

[41]See Notification of Electronic Health Records (EHR) Standards 2016 for India, MoHFW Circular No. Q-11011/3/2015-eGov(30/12/2016),availableathttps://mohfw.gov.in/sites/default/files/17739294021483341357.pdf, accessed on 21/05/2021

[42]Electronic Health Record Standards, 30th December, 2016, https://www.nhp.gov.in/NHPfiles/EHR-Standards-2016-MoHFW.pdf accessed on 21/05/2021

Minister Shri Narendra Modi launched the National Digital Health Mission, guided by those as mentioned above National digital health blueprint. India also has the Personal Data Protection (PDP) Bill, which has conflicting provisions to DISHA on matters relating to healthcare.

A digital implementation framework for the Pradhan Mantri Jan Arogya Yojana (PMJAY) scheme was launched to grant healthcare access to 50 crore people in the country. The E.H.R. system was proposed to use.[43]Implementing E.H.R. in different data points, which can be accessed at other places through standardization and interoperability, brings high credibility and comprehensiveness to the recorded data. For the speedy implementation of the E.H.R. system, the government should incentivize adopting the new system leaving behind their legacy software. Instead of going with private server options, the software developers also should try to make use of the technologies and shall adopt cloud-based E.H.R. solutions that could reduce the cost and at the same time increase efficiency. To a certain extent, Indian healthcare centres are implementing EHR/ EMR, especially in private sector hospitals, as per WHO's requirements. The international Statistical Classification of diseases and related health problems -many hospitals are implementing the 10th version to understand the morbidity and mortality rates.[44]

At the same time, certain factors influence the successful implementation of Electronic Health Records in India. Any guidelines that the Govt of India brought collectively apply to both urban and rural areas. All we have already discussed above, in a country like ours where there exists a considerable difference in a rural and urban healthcare scenario, there are certain factors that the authorities need to look into for successful implementation of the Digital Health Records.

Firstly, the difference in technological advancements seen in urban and rural health centres, whether public or private, can impact the successful implementation. The majority of the publicly-owned health centres in rural areas lack adequate technological infrastructure, trained staff, or even proper awareness. Even in urban areas, it takes time to integrate their systems into the new network when it comes to cloud-based electronic health record systems. This is one of the fundamental and most adverse problems any institution is going to face.

[43]See National Health Stack: Strategy and Approach, NITI Aayog, Government of India, available at https://niti.gov.in/writereaddata/files/document_publication/NHS- Strategy-and-Approach-Document-for-consultation.pdf accessed on 21/05/2021

[44]. Kumar, A., Jeyalakshmi, S., Mukhopadhyay, K.P. & Gupta, P. (2004). *Improving and strengthening the use of ICD 10 and medical record system in India.* Central Bureau of Health Intellegence, New Delhi. Retrieved from: http://www.cbhidghs.nic.in/writereaddata/mainlinkfile/Combined10.pdf, accessed on 15 May 2021

Letting go of the existing status quo and moving on to an entirely new complex system, in the first place, will take a lot of time to adapt, and the migration period will also be too high.

Secondly, the Rural-Urban healthcare divide is the primary concern that's haunting a country like India. We have seen epidemic diseases spreading like wildfire due to the high population we have; at the same time, it needs to be monitored and treated effectively- which remains a distant dream. Even today, in rural areas, patent records are kept in paper-based systems and are not fully implemented. The cost of standardization and implementation will also be a considerable burden upon the state, and wherein in most case scenarios, the system has to be built from scratch.

Thirdly, though internet penetration has shown a significant leap in the last decade, we are lagging when compared to other developed countries. The Internet penetration rate in India went up to nearly around 45 percent in 2021, from just about four percent in 2007. Although these figures seem relatively low, it meant that almost half of the population of 1.37 billion people have access to the internet.[45] When it comes to active internet users, India has become the second-largest market with 504 million active users(first being China), of which 227 million are from rural India and 205 million are from urban areas. Seventy-one million kids whose ages range from 5-11 go online using adult devices.[46] The above data is from November 2019 and is expected to accelerate due to the new online culture that the covid -19 pandemic has brought in. But when it comes to internet penetration, India stands at 45%, which is way behind the U.S.A. and China. But when we opt for a complete digital health transformation, it needs to be accessible by all fractions of society. The pandemic has set the suitable ground for experimenting with digital transformation in the healthcare sector. The concept of a properly regulated E.H.R. system will play a crucial role in evolving the Indian healthcare scenario.

In a country like India, adopting a standardized digital health system and properly regulated Electronic Health Record systems can bring ground-breaking changes to the healthcare scenario. But when we move to an entirely new model, proper awareness has to be given to even the lower strata of the society, or else this can be detrimental to the whole country. There can be fraudsters and other unqualified professionals who can easily penetrate the new model and exploit the country's rural and uneducated majority. Currently, our National

[45]Sandhya Keereli, *Internet penetration rate in India from 2007 to 2021*, 27th April, STATISTA, https://www.statista.com/statistics/792074/india-internet-penetration-rate/, accessed on 15 May 2021

[46]Digbijay Mishra & Madhav Chanchani, *For the first time, India has more rural net users than urban*, published on May 6th 2020, TIMES OF INDIA, https://timesofindia.indiatimes.com/business/india-business/for-the-first-time-india-has-more-rural-net-users-than-urban/articleshow/75566025.cms accessed on 22nd May,2021.

Digital Health mission is rolling out in a phase to phase manner, and people in Andaman & Nicobar Islands, Chandigarh, Dadra & Nagar Haveli and Daman & Diu, Ladakh, Lakshadweep, and Puducherry can currently apply for their voluntary Health ID's, which is voluntary. India adopts a pragmatic agenda of "Think Big, Start Small, Scale Fast."

As part of its national e-Governance ambitions, the Government of India (GoI) has notified several standards to promote interoperability and seamless exchange of data and services between systems. The development of countrywide standards is made possible through the collaborative efforts of stakeholders such as the Department of Information Technology (D.I.T.), the National Informatics Centre (N.I.C.), the Standardization Testing and Quality Certification (STQC), and other government departments and agencies. In addition to healthcare, these standards are broadly relevant in different eGovernment programs around the country.

The Ministry of Health and Family Welfare (MoHFW) announced the Health Data Management Policy, 2020 (HDM) in August 2020 to digitize the whole Indian healthcare ecosystem.[47] In 2017, the government released the National Health Policy and the resulting National Digital Health Blueprint (NDHB), both of which were intended to complement the overall vision of the government by developing an enabling and interoperable digital framework to support universal health coverage while also ensuring the security of sensitive personal medical data of citizens. The National Digital Health Board (NDHB) suggested creating a new institution known as the National Digital Health Mission (NDHM), which would be a completely governmental agency with total functional autonomy.

HDM incorporates the concept of "Security and Privacy by Design" and is intended to serve as a guiding document for the entire National Digital Health Eco-system (NDHE). It also establishes the minimum standards for data privacy protection that should be adhered to by all parties involved in the NDHE. According to Article 2, HDM applies to all entities involved in the NDHM and partners of the NDHE, including, for example, (i) entities and individuals who have been issued an I.D. under the Policy; (ii) healthcare professionals; (iii) relevant professional bodies and regulators; (iv) health information providers; and (v) any health care provider who collects, stores, and transmits health data in electronic form.

[47]The draft stage and will be finalized after receiving suggestions from members of the general public.

The HDM is consistent with the Personal Data Protection Bill in terms of the scope of personal or sensitive personal data collected and processed, the control of data principles over the same, the appointment of a data protection officer, the requirement for clear and conspicuous privacy notices, and the information requirements associated with those notices and requirements. The HDM, under Article 14, provides the data principal various rights concerning the data gathered, including the right of confirmation and access, rectification and deletion, restriction of disclosure or objection to disclosure, and data portability, among other things.

Article 15 of the HDM envisions the establishment of a system for health identification. Data principals have the option of requesting the establishment of a free Health ID, which will allow them to participate in the NDHE and have their personal information linked to their Health ID, which will recognize the data principal as the owner of any personal information provided with the NDHE. According to the provisions of this HDM, the Health ID is designed to serve as a single point of reference for all instances of data collection and processing conducted in line with its terms. Aspects covered in Chapter V of HDM include the responsibilities of data fiduciaries about the processing of personal data, as well as the foundations upon which any collection of personal data should be based. These foundations include accountability, transparency, privacy by design, choice and content-driven sharing [48], purpose limitation (including data quality), data collection, use, and storage limitation (including collection, use, and storage limitation).

The practice of telemedicine, on the other hand, has sparked some controversy. Because of a lack of defined rules, registered medical practitioners are faced with substantial uncertainty, which has led to concerns about the use of telemedicine. Because there is no proper structure in place, the 2018 judgment of the Hon'ble High Court of Bombay [49]has generated doubt regarding the position and validity of telemedicine in the Indian healthcare system.

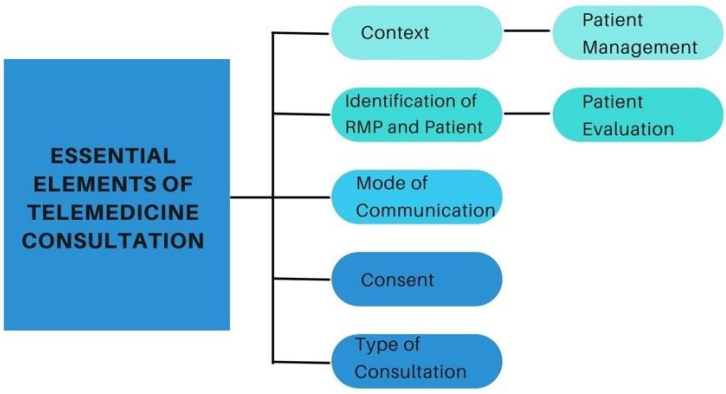
In the end, on March 25, 2020, the Telemedicine Guidelines 2020 (Guidelines) formulated by the National Institute of Transnational Information Technology and Governance (NITI

[48]Data protection requirements shall be considered as part of the implementation and design of the systems, products, and business practices by the data fiduciaries.
[49]Deepa Sanjeev *Panicker&Ors v. State of Maharashtra* ,Criminal Anticipatory Bail Application No. 513 OF 2018

Aayog) were notified under the Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulations (Ethical Guidelines). The Guidelines lay down the norms for the doctor-patient consultations via phone, video, and chat applications, including telemedicine platforms and WhatsApp, in addition to holding doctors accountable to patients for providing teleconsultation following the Guidelines, which include a list of dos and don'ts for physicians. Telemedicine, according to the Guidelines, is defined as "the delivery of health care services, where distance is a critical factor, by all health care professionals who use information and communication technologies for the exchange of valid information for the diagnosis, treatment, and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interconnected network environment."[50]

As per the new guideline, doctors should keep track of their patients' responses to teleconsultations: In India, doctors do not often keep patient records for in-person O.P.D. Appointments since they are not required to do so. The prescription is completed with the appropriate medical history, observations, and findings, and it is then given to the patient to complete. When using teleconsultation, doctors are required to prepare, maintain, and preserve the patient's records (including case history, investigation reports, images, and other relevant information), a copy of the prescription issued, and proof of teleconsultation (including phone call history, email records, chat/text record, video interaction logs, and other relevant information). While no specific period is specified for how long such documents must be kept on file, it is typically advised that they be held for three years after they are created.

[50]Telemedicine Guidelines, 2020



Source: sciencedirect.com (Internet)

It's an undisputed fact that maintained health records during telemedicine can be done effectively only through Electronic Health records. But the proper implementation and effective standardization are required for quality telemedicine service. The new guideline was an immediate response to the unprecedented Covid-19 pandemic, and therefore it's not clear how the health data has to be maintained or preserved. New and detailed regulations are required in the telemedicine sector, which should be framed taking into comparison other international standards,

2.6 CONCERNS IN EHR

When things go digital, it always poses several challenges and obstacles. The same is the case with E.H.R.s. The adoption of E.H.R.s is not as easy as it sounds. It requires an enormous amount of digital and technological support. The importance of synchronization and storage of data increased the adoption of E.H.R.s in the health care sector.[51] Since 2012, the adoption rates of E.H.R.s have been relatively high across the globe. For example, in Sweden and Germany adoption rate was more than 80%, the United States accounted for 69%, and Canada over 56%.[52] Although E.H.R.s have the potential to improve the quality of care, reduce medical errors, and lower administrative costs, incorporating them into clinical practice will require significant investments in technology, in addition to changes in existing

[51] *Comparing Usability Testing Outcomes and Functions of Six Electronic Nursing Record Systems*, NATIONAL CENTER FOR BIOTECHNOLOGY INFORMATION (2016), https://pubmed.ncbi.nlm.nih.gov/26878766/, accessed on 20 May 2021

[52] *A Survey of Primary Care Doctors in Ten Countries Shows Progress in Use of Health Information Technology, Less in Other Areas*, (2017), HEALTH AFFAIRS, https://www.healthaffairs.org/doi/abs/10.1377/hlthaff.2012.0884, accessed on 20 May 2021

systems and processes.[53] Even after having considerable potential benefits from the usage of electronic records, it may not be feasible for every country, every medical institution to implement the same due to the cost constraints, standardization limits, and technical limits.

While implementing E.H.R.s, one has to make sure that the quality of those services is not compromised at any cost. Every web-based project experience, including these records, requires crucial scrutiny for their confidentiality, costs, and liability risks. Other concerns include the lack of well-trained clinician informatics to lead the workforce and health information data standards.[54] Therefore, the major obstacles that lie in the way of full-fledged implementation of electronic records can be shortened as follows:

- In the age of web-based data storage and information, confidentiality, security, and privacy pose the first challenge. Every time, it may not be possible to keep a check on who can access the data. With the implementation of high-standard policies and regulations that limit the use and disclosure, informational privacy can be kept intact.
- The products required for implementing E.H.R.s require an enormous investment and capital, i.e., it is costly.
- The standardization of electronic records is still in a dilemma. This is mainly due to the inadequate rules, standards, guidelines, and policies governing digital health records. For example, there is no single exclusive regulatory framework in India other than the I.T. Rules, 2011, which very limitedly controls sensitive personal data and information. Only with implementing the proper regulatory framework, the business organization would come forward to implement electronic records within their system.
- At the initial stage, it may affect the workflow, thereby reducing the practice productivity of the concerned organizations, hospitals, and medical practitioners.
- The human resource that can lead the workforce of electronic records may not be well aware of all the technical aspects surrounding the same. As technology keeps updating day by day, it may not be possible for the technicians to be updated regularly. Functional training is required for the personnel so that they use the technologies effectively.

[53]SimaAjami, *Barriers to Implement Electronic Health Records,* NATIONAL CENTER FOR BIOTECHNOLOGY INFORMATION, (2013), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3804410/, accessed on 20 May 2021
[54]Ibid

- Ownership concerning the data generated is an important aspect that needs to be looked into. Since sensitive personal data will be stored as electronic records, it is necessary to decide as to who has the ownership w.r.t. data stored, whether it is the data generator (hospitals and health care institutes) or the patient himself. In some instances, these health care institutes may make potential use of the data for medical researchers in the capacity of the data owner.

The foremost significant challenge in the implementation of E.H.R.s is confidentiality and privacy concerns. Electronic records must always satisfy its users against privacy, security, and confidentiality.[55] If personal records of patients end up in the hands of a person who is not authorized could result in identity theft, affecting the individual's credit and reputation. There is also a high risk of misplacement and mismanagement of data. This necessarily goes in parallel with the regulatory and governance structure of the country where it is implemented. To secure the confidentiality and privacy of the data, there must be a proper legal framework to govern the same. The regulatory framework also looks into the role of setting up standard policies, rules, and regulations.

The second challenge is seen in the adoption stage, i.e., the cost of implementation of any digital health records is high. There is a relative uncertainty to the expenses linked to electronic health initiatives and their allocation.[56] E.H.R.s require high interoperability standards to facilitate the sharing of data across multiple operators. The cost of adoption of such standards is always high. Only those hospitals having access to high monetary resources would be in a position to adopt the same. Hence, the cost of implementation always stands as a barrier to the adoption of E.H.R.s. At the global level, there are no incentives to encourage the private parties to get into electronic records.

The third challenge is the lack of a proper human workforce to lead the technical incorporations into the health sector. Only if the technicians are well trained and equipped with modern technologies will they be better positioned to implement the same. There must be a supervisory authority to review the works undertaken by such technicians. And there are

[55]Terry NP, *Privacy and the Health Information Domain: Properties, Models and Unintended Results*, 10 European Journal of Health Law, 223-22, 2010.
[56]Tracy D Gunter, Nicolas P Terry, *The Emergence of National Electronic Health Record Architecture in the United States and Australia: Models, Costs and Questions*, Journal of Medical Internet Research, 14th March 2018, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1550638/, accessed on 20 May 2021

no qualifications prescribed as to who can undertake the implementation of electronic health records. The critical question that needs to be answered is whether all the hospital authorities are in a position to implement electronic health records for data storage.

The present is the age of data and information, and the rapid technological progress has changed every area of life and work. So, with the outset of advancements in information and technology, the health care sector started to shift to a new paradigm, including electronic records. This shift is a very appreciable effort that made easy access to information and regular updates of data. Even if it may be costly at the initial stage, it is always a much-needed change for the long time run. In the health sector, information has a crucial role in the planning, evaluation, training, research, and legal aspects. Every set of data and information is valuable, and it must be well documented, maintained, retrieved, and analyzed.

2.7 CONCLUSION

The primary reasons for implementing an electronic health record system are to facilitate patient care and improve the quality of that care. Accurate and timely health information that is readily available to both providers/users and consumers has significant benefits for the healthcare of all people and would improve the community's health and welfare. Additionally, it will increase healthcare professionals' productivity in delivering care and offer a solid foundation for clinical and health service research.

According to some, the use of E.H.R.s will revolutionize how we gather, store, and utilize health information. Patients are anticipated to become increasingly engaged in healthcare decision-making when electronic technologies make information about their health issues and treatment readily available and accurate. It is frequently argued that healthcare practitioners deliver better care because they can more efficiently communicate up-to-date information about a patient's healthcare to other healthcare providers involved in the patient's care and better access to best practices and the latest research findings.

3. CHAPTER 3: HEALTH DATA PROTECTION – A COMPARATIVE ANALYSIS

3.1 INTRODUCTION

Digitizing health records benefits patients and hospitals by streamlining the process of keeping and monitoring treatment and plans. Digitizing health records begins with the gathering and recording of patient data at multiple data collection sites. Hospital front offices, clinics, diagnostic centres, and healthcare equipment that generate patient-specific data can all serve as collecting locations. These data are then stored in the collecting points' storage repositories for further processing and future usage. With the proliferation of data repositories and the advancement of technology, the risk connected with data is increasing. With digital health data, care must be taken to secure the data's security and safeguard the patient's privacy and confidentiality. In the healthcare setting, patient confidentiality and privacy protection are critical components of the doctor-patient interaction. It is crucial to enable the secure transfer of interoperable health records when patients seek treatment from multiple health care providers.

One of the advantages of digital health is that it enables health information exchange to ensure care continuity. This sharing, in turn, raises the spectre of privacy violation. As part of the ethical requirement to "first, not harm," healthcare practitioners are obligated to maintain the confidentiality of patient information, as revealing it might result in highly significant harm, regardless of whether the information concerns "sensitive" topics such as mental or sexual health.

Privacy may be protected by implementing proper rules, data management practices, and technology protections. Potential dangers to privacy in digital health include the following:

- Theft, loss, damage, or destruction/modification of health information
- Compromised access to health record systems
- Violations of security and privacy rules

Earlier, the patient owned their medical records and had the right to examine her documents, learn about the conditions governing access, and modify or cancel the consent already granted. Consent is a necessary component in ensuring the privacy and confidentiality of the patient's data. Consent is sought for various reasons, including authorization to undertake

healthcare activities, disclosure of why, what, and how health information is gathered, and permission to participate in clinical studies. Additionally, it encompasses the exchange of health data for the sake of referral and research. Each healthcare provider should monitor and maintain rules regarding patient permission and access.

But now, the patient has virtually no access to their integrated electronic healthcare records. As she receives care from several experts, a patient's clinical, pathology, and imaging records are dispersed across multiple locations. This makes accessing the documents more difficult for the patient. This may be made considerably more difficult by the usage of disparate programs, platforms, and file formats, as well as disparate levels of data quality, interoperability, interchange, and access.

The following is a comprehensive overview of the difficulties associated with safeguarding patients' privacy in electronic health records:

- Managing individual participation rights
- Managing accountability and access control
- Administration of cases and legal considerations
- Application of privacy policies holistically across public and private sector healthcare providers
- Cross-border data transfers
- Regulatory mechanism for data control

To address the issues at hand, we categorize them into two categories. The first can be controlled and resolved via government-provided laws and regulations. In contrast, the second may be managed and resolved through information technology and data management policies.

This chapter addresses several privacy and security problems associated with health data protection and will analyze the legal framework that various global nations have adopted to address the same.

3.2 HEALTH DATA PROTECTION LAWS IN DIFFERENT COUNTRIES.

The proposed legal and policy frameworks for health data protection in India are at a crossroads. It is imperative that the government first design and execute a robust, patient-centered legal framework before spending on the conversion to electronic health records. It can be done only through proper analysis and observation of various global frameworks regulating Electronic Health Records (EHRs). This chapter shall discuss the regulatory framework for EHR in the USA, EU, and Australia.

3.2.1. POSITION IN EUROPEAN UNION (EU)

Generally, data protection regulations strive to regulate 'personal data' about persons or 'data subjects' by data processors' and 'data controllers.'[57]Notably, not all information about a person is subject to data protection regulation, as the only information that directly affects an individual's privacy is considered 'personal.'[58]The controller (or the processor designated by the controller to process the data) is accountable for how personal data about an individual is treated. [59]

The EC Data Protection Directive serves as the foundation for numerous national data protection laws in the EU Member States, establishing eight data protection principles for states implementing the Directive.[60]The fundamental premise of data protection is the lawful and equitable processing of personal information. [61] The data must be collected for defined and legitimate purposes and pertinent to the processing purpose.[62] Data should not be retained for any longer than is necessary to accomplish the stated goal. [63]Additionally, both the controller and processor are required to include suitable technical and organizational safeguards to protect against unauthorized processing.[64] The processor is subject to the same strict conditions as the controller, who must also monitor the processor's compliance with the security measures throughout the agency's lifetime.[65]

[57] Data Protection Act, 1998, §1(1), c. 29 of 1998, Acts of Parliament, 1998 (UK). (This implementing legislation ensures compliance with the data protection principles enunciated in the Data Protection Directive).

[58] Durant v. Financial Services Authority, 2003 EWCA Civ 1746. (This case defines data as 'personal' only if it 'affects his privacy'. According to Durant, information should be (i) 'biographical in a significant sense' and (ii) second, the focus should be on the data subject, excluding information held by the data controller that contains a passing reference to particular individuals).

[59]UK Data Protection Act, 1998, §1(1), c. 29 of 1998, Acts of Parliament, 1998 (UK). (This provision "data controller" means, subject to sub- section (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed).

[60] UK Data Protection Act, 1998, Schedule I, c. 29 of 1998, Acts of Parliament, 1998 (UK). (Data Protection Directives are part of the Council of Europe's attempts to harmonise national laws on data protection in its 1973 and 1974 resolutions).

[61] UK Data Protection Act, 1998, Schedule 2 and 3, c. 29 of 1998, Acts of Parliament, 1998 (UK). (Conditions for fair and lawful processing of personal data include (i) obtaining the patient's consent and (ii) that data must be processed in the patient's 'vital interests').

[62] UK Data Protection Act, 1998, Schedule 1, Part 1, Principles 2 and 3, c. 29 of 1998, Acts of Parliament, 1998 (UK).

[63] UK Data Protection Act, 1998, Schedule 1, Part, Principle 5, c. 29 of 1998, Acts of Parliament, 1998 (UK).

[64] UK Data Protection Act, 1998, Schedule 1, Part I, Principle 7, c. 29 of 1998, Acts of Parliament, 1998 (UK). (Appropriate technical and/or organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data)

[65] P. ROOM & F. F. WATERHOUSE, BUTTERWORTHS DATA SECURITY LAW AND PRACTICE 68 (Butterworths Law, 2009).

Additionally, the Directive establishes a general presumption against the adequacy of third-country data protection laws.[66] Where data is transferred between States that have complied with the Directive by enacting similar domestic legislation, the data controller (the person in possession of the information) can be assured that the target country's level of protection matches that in the host State.[67] However, where data is transferred between a Member State and a third country, the third country's level of protection will be considered in light of the surrounding circumstances, such as the nature of the data and the purpose and length of the proposed processing activity.[68]

The regulation limits the use of health data to three purposes:

- Data may be processed in the course of medical diagnosis, treatment of healthcare services, and the administration of preventative medications, as well as in other instances when healthcare professionals process data.
- The data may be processed for reasons of public interest, such as guaranteeing a high standard of quality for medical goods, safety, or services. The data may be processed in the event of real cross-border risks to health.
- The data may be processed in the public interest, such as social protection.

The regulation established that implicit consent is insufficient for sensitive personal data and that explicit consent is necessary. This is due to the inherent inequity between the data subject and the data controller. For instance, the patient and the hospital or life sciences business that is performing the research. The regulation establishes a timeframe for patients to request their data be destroyed once their treatment is complete or discharged. If this information is not destroyed, it may become vulnerable to illegal access and misuse. This is a critical step in the establishment of a privacy-protective ecosystem.

Another additional problem is the type and scope of permission. Consent obtained during a clinical study is not always sufficient to conduct subsequent research.

In 2008, the European Court of Human Rights ('ECtHR') stressed the critical nature of preserving an individual's health data in *I v. Finland*.[69] The case involved an employee of an

[66] Data Protection Directive, Article 25 and 26.

[67] E. MOSSIALOS, G. PERMANAND, R. BAETEN & T. K. HERVEY, HEALTH SYSTEMS GOVERNANCE IN EUROPE: THE ROLE OF EUROPEAN UNION LAW AND POLICY 564 (Cambridge University Press, 2010).

[68] Id

[69] I v. Finland, Application No. 20511/03: 2008 ECHR 623. (The ECHR stated (upholding the Court's previous decision in Z v. Finland, (1988) 25 EHRR 371) that the protection of personal data, in particular medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as

eye clinic who was formerly a patient, and whose HIV status became known to her co-workers as a result of her colleagues' open access to the patient record, which contains information on diagnosis and treatment,[70] The ECtHR stated in the case that due to the "sensitive nature of this sickness," the obligation of confidentiality would be especially crucial in the applicant's case.[71] The ECtHR's observation imposes a responsibility on data controllers to safeguard any private data against unauthorized access.[72]

3.2.2. POSITION IN UNITED STATES OF AMERICA

Until now, the United States of America USA has taken a sectoral approach to data protection law. Currently, the United States of America lacks explicit legislation governing the acquisition and use of personal information at the federal level. Indeed, while the US Constitution makes no express reference to a 'right to privacy,' many industries have developed overlapping protections. The following policies governing health information and privacy are examples of this issue.

US government and other organizations such as the Institute of Medicine (IOM) have been promoting the adoption of EHRs to enhance the quality of health care. Cost, organization, standards, functionality, and interoperability have all delayed the EHR's growth. Independent groups and the federal government have used committees, studies, and guidelines to pave the way for increased adoption of EHRs.

The Health Insurance Portability and Accountability Act (HIPAA) were enacted in 1996 to create accountability standards and criteria for the security and confidentiality of electronic health information. The early development of EHRs was influenced by the HIPAA regulations, which first controlled Practice Management Systems. Numerous organizations and government agencies have asked for more action to aid in promoting and establishing EHR standards. Consolidated Health Information (CHI) took the next important step in 2003 when it issued EHR standards. The United States Department of Health and Human Services (DHHS) commissioned the nongovernmental organization known as the Certification Commission for Health Information Technology (CCHIT) to accredit EHR projects in 2005.

---

guaranteed by Article 8 of the European Convention on Human Rights. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention).

[70] ROOM & WATERHOUSE, *supra* note 9, at 27

[71] *Id*

[72] ROOM & WATERHOUSE, *supra* note 9, at 31

Other government agencies have continued to encourage the adoption of EHRs and assist healthcare providers in implementing these initiatives to improve patient care.

HIPAA was enacted in response to the digitization of data in the United States' health care business and growing anxiety about the privacy and security of personal health information. HIPPA sets national security standards for the 'use' of such health information and privacy rules to protect such health information.[73] After a while, the Health Information Technology for Economic and Clinical Health Act of 2009 ('HITECH')was enacted in 2009 to promote the effective use of technology to facilitate the exchange of personal health information. It required patients and the US Department of Health and Human Services (hence referred to as 'HHS') to receive a 'notice' in the event of a breach of unsecured and protected health information.

As a result, the HHS adopted the 'Privacy Rule'[74]and the 'Security Rule,' which established some individual rights and imposed stringent restrictions on the use and distribution of health information. Both of these measures ultimately set a federal minimum standard of privacy protection for health information.

HIPAA and HITECH, which together constitute the important health privacy and security statute in the United States, are inherently self-contradictory. These regulations and the HHS regulations apply solely to organizations and entities that meet the criteria of a 'covered entity.'[75] Within the meaning of HHS regulations, a covered entity is defined as follows:

a) A medical insurance policy;
b) A clearinghouse for healthcare information;
c) A provider of health care who is capable of electronically communicating personal health information.

This means that consumers are unaware of their health data. They never know when their information is protected and when it is not, owing to the overlapping and contradictory patchwork of current regulations, under which specific privacy laws control particular facets of the United States' healthcare system.[76]However, these distinct components have proven critical in ensuring health data security and facilitating the gathering and sharing of data.

---

[73]INSTITUTE OF MEDICINE, BEYOND THE HIPAA PRIVACY RULE : ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH (National Academies Press 2009)

[74] General Administration Requirements, 45 C.F.R. §160 (2016), HIPAA Security and Privacy Regulations, 2018, §§160.101 and 164.104.

[75]COVERED ENTITIES AND BUSINESS ASSOCIATES, US DEPARTMENT OF HEALTH AND HUMANS SERVICES, https : //perma.cc/4SWX-KLBH (last visited 30th June 2021).

[76] Nuala O'Connor, *Reforming the US Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELATIONS, (Jan. 30, 2018) https : //www.cfr.org/report/reforming-us-approach-data-protection

Regulations promulgated by HHS under HIPAA are commonly referred to as the Privacy and Security Rules[77]. HIPAA was modified in 2009 by the Health Information Technology for Economic and Clinical Health Act (HITECH) and updated in January 2013 with the release of the Omnibus Final Rule by the Department of Health and Human Services (HHS).[78]

The HIPAA Privacy, Security, and Breach Notification Rules, as updated by the HIPAA Omnibus Final Rule[79] in 2013, set forth how certain entities, including most health care providers, must protect and secure patient information. They also address Business Associates (BAs) responsibilities, including EHR developers working with health care providers. While the Privacy Rule[80]covers all "individually identifiable health information[81],the Security Rule[82] exclusively protects electronically protected health information (ePHI) and is the basis of the Federal data breach regulation.[83]

ePHI is a term that refers to electronically recorded, personally identifiable health information about an individual. [84]These records are kept in health information systems (HIS) in hospitals, research institutions, and diagnostic laboratories worldwide.[85] The Security Rule categorizes dangers posed by exploiting HIS vulnerabilities into three categories: physical, administrative, and technical. [86]

[77]See 45 C.F.R. §§160, 162, 164 (2016).
[78]See General Administration Requirements, 45 C.F.R. §160 (2016) and Security and Privacy, 45 C.F.R. § 164 (2016).
[79]In January 2013, HHS issued a Final Rule that modified the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Genetic Information Non-discrimination Act (GINA). This Final Rule is often referred to as the HIPAA Omnibus Final Rule. These modifications are incorporated throughout this Guide. The Rule can be accessed at http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdfhttp://www.cms.gov/RegulationsandGuidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms/
[80]The HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html, (last visited on July, 14th 2021).
[81]See 45 C.F.R. § 160.103 (2016).
[82]The Security Rule, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html, (last visited on July 14th 2021).
[83]See 45 C.F.R. § 164.306(a)(1) (2016).
[84]See Integrating Privacy & Security into Your Practice, HEALTH IT, https://www.healthit.gov/providers-professionals/ehr-privacy- security/practice-integration (last accessed on August 21, 2021).
[85]Shahidul Islam Khan, Abu Sayed &Latiful Hoque, Digital Health Data: A Comprehensive Review of Privacy and Security Risks and Some Recommendations, 24 COMPUTER SC. J. OF MALDOVA 273, 274 (2016).
[86]See 45 C.F.R. § 160 (2016); see also 45 C.F.R. § 164

3.2.2.1. PHYSICAL SAFEGUARDS[87]

Physical safeguards are standards for "buildings and equipment" and the dangers presented by "natural and environmental causes" as well as illegal human physical access.[88]Notably, "data backup and storage" is described as "addressable."[89] Healthcare organizations are required by this implementation standard to "make a retrievable, precise duplicate of electronically protected health information, if needed, before equipment transfer."[90] Additionally, the "addressable" requirements cover facility security planning, access control, and validation, which are also promulgated with broad wording.[91]

3.2.2.2. ADMINISTRATIVE SAFEGUARDS[92]

Administrative safeguards are the "nontechnical policies and procedures that an organization's management develops on appropriate employee behaviour, personnel processes, and proper technology use inside the company."[93] The security management procedure is the most critical requirement needed by the administrative safeguard.[94] Organizations should analyze possible data security risks and "take security measures adequate to limit risks and vulnerabilities to a reasonable and suitable level."[95]This section contains two accessible implementation specifications: “access authorization "as well as "access establishment & modification."[96] Under these regulations, healthcare providers are urged to implement policies defining and restricting access to their HIS data.

Additionally, the standards under the category Security Awareness and Training are accessible for this.[97] This implies that healthcare providers have considerable freedom over how they operate as a top-to-bottom organization, including who gets access to what data in their HISs.[98] Despite knowing that employee negligence contributes to data security concerns, HIPAA grants healthcare companies considerable discretion over authorization-related protections.

---

[87] ThePhysicalSafeguards,http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf, (last visited on July 30th 2021)

[88]MARGARET AMATAYAKUL, HANDBOOK FOR HIPAA-HITECH SECURITY 84 (American Medical Association 2013)

[89]See 45 C.F.R. § 164.310(d)(2)(iv) (2016).

[90]See 45 C.F.R. § 164.310(d)(2)(iv) (2016).

[91]See 45 C.F.R. § 164.310(a)(2)(ii) (iii) (2016).

[92]http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf

[93]See 45 C.F.R. § 164.304 (2017) (defining "administrative safeguards").

[94]See 45 C.F.R. § 164.308(a)(1)(i) (2016).

[95]See 45 C.F.R. § 164.308(a)(1)(ii)(B) (2007).

[96]See 45 C.F.R. § 164.308(a)(4)(ii)(B) (C) (2007).

[97]See 45 C.F.R. § 164.308(a)(5)(i) (a)(5)(ii)(D) (2007).

[98]HIPAA Security Series: Part2, U.S. DEP'T OF HEALTH & HUM. SERV., 9 (March 2007), https://www.hhs.gov/sites/default/files/ocr/ privacy/hipaa/administrative/securityrule/adminsafeguards.pdf

3.2.2.3. TECHNICAL SAFEGUARDS[99]

Technical safeguards are a set of adaptable criteria for the functioning of HISs that "hold, process, or transmit electronically protected health information."[100]Among the protections that might be addressed in this section is the need for healthcare institutions to "establish a system for encrypting and decrypting electronically protected health information."[101] This clause contains no further information, such as distinguishing between data at rest and data in transit or a minimum degree of encryption. In other words, the HIPAA-mandated technological protections make no distinction between data that is "moving" through a network—private or public—and data that is kept in some form (or "at rest").[102]Encryption is referenced once again in section 312(e)(2) (ii).[103]When a healthcare institution "deem[s] [it] suitable, data should be encrypted.[104]The mandated minimal level of technical protections to protect HISs and ePHI from cyber-threats is simply too low across the board. As a result, attacks like ransomware have wreaked havoc on the healthcare business.

It is essential to have robust cybersecurity practices

in place to protect patient information, organizational assets, your practice operations, and your personnel. Of course, to comply with the HIPAA Security Rule[105], cybersecurity is needed whether you have your EHR locally installed in your office or access it over the internet from a cloud service provider.

3.2.2.4. THE DANGERS OF PHARMACEUTICAL MARKETING

In the United States, HIPAA intends to boost the healthcare system's efficiency and effectiveness by supporting the creation of a health information system through the adoption of standards and procedures for the electronic exchange of specific health information.[106]

At various stages of data collection, processing, and disclosure, patient privacy can be protected.[107]De-identified data collected at the point of collection may be used to maintain patient anonymity. Additionally, the spectrum of justifiable reasons for personal data

---

[99]Covered Entities and Business Associates, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html, (last visited on 30th July 2021).
[100]45 C.F.R. § 164.304 (2017) (defining "technical safeguards" as "the technology and the policy and procedures for its use that protect electronic health information and control access to it.").
[101]45 C.F.R. § 164.312(a)(2)(iv) (2007).
[102]45 C.F.R. § 164.312(a)(2)(iv) (2007).
[103]45 C.F.R. § 164.312(e)(2)(ii) (2007).
[104]45 C.F.R. § 164.312(e)(2)(ii) (2007).
[105]Administrative Security Rule, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/, , (last visited on 30th July 2021).
[106]Health Insurance Portability and Accountability Act, Pub. L. 104-191, §261.
[107]N. P. Terry, *Symposium: The Politics of Health Law: Under-regulated Health Care Phenomena in a Flat World: Medical Tourism and Outsourcing*, 29 W. N ENG. L. REV. 441 (2007).

acquisition may be limited to specific purposes, such as treatment.[108] As a result, informational privacy ensures that personal information is not shared with corporate entities. However, as healthcare delivery systems evolve and the physician-patient interaction gets more complex; however other interested parties are establishing a firmer foothold in the healthcare system.

Concerns about the aggregation of patient information do not appear exaggerated in light of the absence of strong permission requirements under HIPAA. The global market for patient data is expanding. Apart from the Food and Medication Administration in the United States, health insurers, researchers, and drug makers make commercial use of prescription data.[109] Because of this, it is not surprising that various state governments have failed to defend legislation prohibiting the sale of prescription data to pharmaceutical companies against challenges by data mining companies asserting that such laws violate their First Amendment rights to freedom of expression.

HIPAA is not the sole federal legislation that regulates health information disclosure. In certain situations, more protective legislation may demand an individual's consent before disclosing health information, whereas HIPAA permits disclosure without authorization. State and local regulations may apply to health care records containing patient information. HIPAA does not pre-empt provisions of state law that are at least as protective as HIPAA. Some examples of such state laws are-

- State Law Requirements for Patient Permission to Disclose Health Information Report[110]
- Access to Minors Health Information[111] etc.

[108] *Id*

[109] E. MOSSIALOS, G. PERMANAND, R. BAETEN & T. K. HERVEY, HEALTH SYSTEMS GOVERNANCE IN EUROPE: THE ROLE OF EUROPEAN UNION LAW AND POLICY 564 (Cambridge University Press, 2010).

[110] Agency for Healthcare Research and Quality, 2009, *Report on State Law Requirements for Patient Permission to Disclose Health Information*. https://www.healthit.gov/sites/default/files/disclosure-report-1.pdf

[111] Agency for Healthcare Research and Quality, 2009, *Report on State Medical Record Access Laws*, https://www.healthit.gov/sites/default/files/290-05-0015-state-law-access-report-1.pdf

3.2.3. POSITION IN AUSTRALIA

In Australia, the Privacy Act, Privacy Act 1988[112], covers the Commonwealth public sector and the national commercial sector, provides additional protection for health information processing by regulating how health service providers acquire and handle personal health information. Even though Australia does not have an absolute right to privacy,' As is the case in the United States, the country has a comprehensive law regulating the right to privacy on a sectoral level.[113]

The Privacy Act applies to all health service providers, including those who only maintain health information. The Act regulates the collection and processing of health information. Because the act is administered by the Office of the Australian Information Commissioner (hereinafter referred to as the 'OAIC'), the Act contains regulations that strike a balance between protecting health information from unintended uses outside of healthcare and advancing public health through medical research. Registrar of Public Records.[114] In lieu of this, the National Health and Medical Research Council has released two legally obligatory sets of guidelines under the Act's Sections 95 and 95A.[115]

The policies cover the following:

(a) Medical researchers must follow processes if personal health information is disclosed to them for research purposes by a Commonwealth institution. [116]

(b) The framework for evaluating requests for organizations to handle personally identifiable health information without the persons' informed permission. [117]

It is important to note that the Privacy Act does not preclude a health service provider from disclosing genetic information with the individual's informed consent; however, in the absence of such consent, the Act permits disclosure of genetic information in limited circumstances, such as when the patient requires health care. [118]

Additionally, where a substantial threat to the patient's genetic relative's life exists and the health service provider complies with the Act's Section 95AA standards.[119]

---

[112]The Privacy Act, 1988, No. 119, Acts of Parliament, 1988 (Australia).
[113]Tanvi Mani, *Privacy in Healthcare: Policy Guide*, The Centre for Internet & Society, (26 Aug, 2014), https : //cis-india.org/internet-governance/blog/privacy-in-healthcare-policy-guide
[114]Australian Government, *Office of the Australian Information Commissioner*<https : //www.oaic.gov.au/privacy/the-privacy-act/health-and-medical-research/
[115]*Id*
[116] The Privacy Act, 1988, §95, No. 119, Acts of Parliament, 1988 (Australia).
[117]The Privacy Act, 1988, §95 A, No. 119, Acts of Parliament, 1988 (Australia).
[118]Tanvi Mani (n 29).
[119]The Privacy Act, 1988, §95AA, No. 119, Acts of Parliament, 1988 (Australia).

3.3 CONCLUSION

Compared to other nations, India has either no facilities or a very inadequate infrastructure for electronic health records, or it is still at a very early stage of development. Only a few private hospitals have implemented an electronic health record system, with the vast majority still relying on handwritten data. As a result, due to a lack of EHR, the data necessary was not obtained. As a result, we must build a functioning EHR that can be hosted in the cloud to protect data transmission and make it available to health organizations for free. Because the creation of the EHR at its foundation is costly, technological efforts may be required to solve these difficulties from the government's side. By utilizing cloud computing, an effective EHR architecture may be created. India does not have an EHR architecture; the government has acknowledged just a few recommendations or projects, and the vast bulk of them are currently under consideration by the government. As a result, we must continue to build on the benefits or approaches of other nations while also recognizing India's successful architecture. To overcome the difficulties, we must concentrate on a few factors that are a hindrance to our architectural design:

1. Provide training to doctors and specialists for them to make good use of the EHR.
2. Adoption of policies and activities that promote standardization.
3. Foster co-operation and collaboration between the private and public health sectors.

Electronic Health Records provide several advantages over traditional paper-based systems, and several nations are placing a high premium on their implementation. EHRs have the potential to be critical in enabling worldwide access and portability of medical records, therefore facilitating international medical treatment. However, there is currently a shortage of globally recognized EHR standards and their implementation. On the other hand, with the growth of health records, privacy concerns are pretty significant. Numerous nations have enacted special privacy and medical legislation to address these issues. However, the right to privacy in healthcare may be applied successfully only through the collaboration of several stakeholders. This covers both private and state institutions, insurance firms, web servers, and civil action groups. As a result, significant worldwide effort is necessary to solve these challenges of EHR privacy and standards.

4. CHAPTER 4: ELECTRONIC HEALTH RECORDS - INDIAN PERSPECTIVE

4.1 INTRODUCTION

Privacy is one of the most fundamental facets of life worldwide, and it is protected by law. In India, it is constitutionally enshrined under Article 21, and India's judicial system has recognized the right to privacy on many occasions. Concerns about protecting personal data and information, in essence, the right to privacy, are persisting. The term "right to privacy" refers to an individual's unique right to manage personal information acquisition, use, and disclosure. While digital health data (DHD) looks to change the Indian healthcare system potentially, online behaviour tracking is about to be adopted without customers' informed permission.[120]Personal information may include but is not limited to personal interests, habits, and activities, family records, educational records, communications records (including mail and telephone), medical records, and financial data.

This chapter will look into the development of India's current legal framework for Electronic health data protection. The chapter shall also analyze different steps that the Indian Government has taken, like Digital Information Security in Healthcare Act (DISHA), Personal Data Protection Bill 2019, Health data Management Policy 2020, etc.

4.1. LAWS RELATING TO MEDICAL RECORDS IN INDIA

According to the Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulations, 2002, every practitioner must keep medical records relating to their indoor patients for three years from the date of the treatment's initiation. If a request for medical records is made, whether by the patient, an authorized attendant, or the legal authorities involved, the papers must be provided within 72 hours. Failure to do so would be considered misconduct. The following are some of the most significant problems that have been addressed:

- Maintain indoor records in a standard proforma for three years after the start of therapy [121]

[120]Fouzia F. Ozair and others, *Ethical Issues in Electronic Health Records: A General Overview*, 6(2) PICR, 44, 44-57, 2015.
[121] Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulations, 2002, § 1.3.1 and Appendix 3.

- A patient's authorized request for medical records shall be acknowledged, and the requested papers should be delivered within 72 hours.[122]
- Maintain a certificate registry that includes all medical certificates issued with at least one identifying mark of the patient and his signature, as well as the complete contents of such certifications.[123]
- It is necessary to make efforts to computerize medical records so that they can be retrieved quickly.[124]

When it comes to retaining medical data in India, there are no specific rules in place. In each case, the hospitals follow their protocol for keeping records for varying lengths of time. According to the provisions of the Limitation Act 1963 and Section 24A of the Consumer Protection Act 1986, which dictate the period within which a complaint must be filed, it is recommended that outpatient records be kept for two years and inpatient and surgical records are kept for three years. The provisions of the Consumer Protection Act, on the other hand, allow for the delay to be excused in suitable circumstances. This implies that the records may still be required even after three years have passed.

The Medical Council of India's rules also requires that inpatient records be kept in a standard proforma for three years after the start of treatment has been completed. In all medico-legal situations, regardless of whether or not a complaint or notification has been received, the documents involved should be kept on file until the case is resolved.

According to the requirements of particular Acts such as the Pre Conception Prenatal Diagnostic Test Act, 1994 (PNDT), the Environmental Protection Act, and others, appropriate preservation of records is required, and such documents must be kept for a length of time stated in the Act. PNDT Act, 1994 stipulates that all papers must be kept on file for a period only until the case is finally resolved, whichever comes first. According to the PNDT Rules, 1996, when records are kept on a computer, a printed copy of the record must be retained once it has been authenticated by the person responsible for the record in question.

The ownership of medical records is a significant source of contention between the patient and the institution receiving treatment. Medical records are, for the most part, the property of

[122] Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulations, 2002, § 1.3.2
[123] Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulations, 2002, §1.3.3
[124] Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulations, 2002, §1.3.4

hospitals, and it is the institutions' the institutions must be in good working order. Medical records must be handled with care by both hospitals and physicians since they may be stolen, altered, and abused for nefarious purposes by anybody interested in the subject matter. As a result, the records should be kept in a secure location. Patients or authorized authorities may request patient records, and it is the hospital's primary duty to preserve and make such information available upon request. However, it is the primary responsibility of the treating physician to ensure that all treatment papers are prepared correctly and signed by the patient. A medical record that has not been signed has no legal standing. The patient or their legal heirs have the right to request copies of their treatment records, which must be given within 72 hours of the request. The hospitals have the right to charge a fair fee for administrative services, such as photocopying papers. Patients' medical records will be considered a failure in service and carelessness if they are not available upon request.

Section 43-A[125] of Information Technology Act, 2004 deals with sensitive personal data or information are liable for damages for negligence in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person. Section 72-A[126] of Information Technology Act, 2004 speaks about disclosure of materials containing personal information of any person by the service providers without the person's consent or in breach of a lawful contract is punishable.

According to Clinical Establishment(Registration and Regulation) Rules, 2010 every clinical establishment is supposed to maintain medical records of the patients treated by it and health information and statistics in respect of national programmes and furnish the same to the district authorities in quarterly formats. Various medical records to be maintained by clinical establishment include[127]-

- Outpatient register
- Inpatient register
- Operation theatre register
- Labour room register
- MTP register(if registered under MTP Act)
- Case sheets
- Medico legal register

[125]Compensation for failure to protect data.
[126]Punishment for disclosure of information in breach of lawful contract
[127]CG 2 Annexe as per Section 12 (1)(iii) of Clinical Establishment (Registration and Regulation) Act, 2010

- Laboratory register
- Radiology and Imaging register
- Discharge Summary
- Medical Certificate in duplicate
- Complaint register
- Birth register
- Death register
- Information in terms of Government programmes
- Number of beds system wise and speciality wise in Clinical establishments providing patient care
- Total discharges

Each category of clinical establishments shall comply with the standard treatment guideline and maintain electronic medical records of every patient as may be notified by the Central government from time to time.[128]

Medical records are admissible in a court of law under Section 3 of the Indian Evidence Act, 1872, as modified in 1961, if they are in the public interest. This kind of documentation is regarded as valuable evidence by the courts since it is widely recognized that facts documented throughout a patient's treatment are accurate and impartial. Medical records written after a patient has been discharged or died do not have any legal significance. Attempting to delete or modify entries is not allowed and may be considered illegal in court. It is recommended that the whole line be scored and reprinted with the date and time if a correction is necessary.

In the following situations, medical records are often requested in a court of law:

- Criminal situations in which the type, timing, and severity of the injuries must be established. It is regarded as critical evidence in establishing the kind of weapon used and the manner of death.
- Cases involving road traffic accidents brought under the MACT Act to determine the amount of compensation
- Employment tribunals in connection to the Workers' Compensation Act
- Insurance claims to establish the length of sickness and cause of death

[128] Clinical Establishment(Registration and Regulation Rules), 2010

Section 91[129] of Code of Criminal Procedure, 1973, regulates targeted access to stored content.

Medical negligence cases may be brought in criminal court if the doctor is charged with criminal carelessness or under the Consumer Protection Act if the doctor's or hospital's treatment is deficient

4.2. LEGAL FRAMEWORK FOR REGULATING ELECTRONIC HEALTH RECORDS IN INDIA

The advancement of information technology in the healthcare industry has enabled the digital preservation and management of patient data at all levels of the healthcare system. The Government of India's support for the Digital India initiative has resulted in numerous breakthroughs in the convergence of the healthcare and information technology industries.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (SPDI Rules) govern the exchange of sensitive personal data between a patient and a healthcare professional, including physical and mental health conditions and sexual orientation, and so on. The Information Technology (Intermediaries Guidelines) Rules, 2011 (Intermediaries Guidelines) regulate organizations that operate as facilitators of electronic health care services to patients in collaboration with independent healthcare experts.

To achieve a "standard-based system for creating and maintaining EHRs," the Government notified the Electronic Health Record Standards in 2016. The new standard came as the successor of the Electronic Health Standards of 2013.These standards address data privacy and security in electronic health records to maintain patient confidentiality. They do not, however, have the legal force of law. According to the EHR Guidelines, data is "individually identifiable" if it contains any identifiers such as a person's name, address (all geographic subdivisions smaller than a street address and pin code), all elements (except years) of dates relating to an individual (including date of birth, date of death, etc.), telephone, cell (mobile) phone and fax numbers, email address, bank account, and credit card information.

The Integrated Disease Surveillance Programme (IDSP) was launched in 2020 to strengthen and sustain a decentralized laboratory-based information technology-enabled disease surveillance system for epidemic-prone diseases. Through trained Rapid Response Teams, it

[129]Summons to produce document or other thing.

tracked disease patterns to detect and respond to epidemics in their early stages of development. IDSP is also managing overall surveillance operations in India for the COVID–19 pandemic. Under IDSP, a near-real-time, web-enabled electronic health information system called the Integrated Health Information Platform (IHIP) was introduced in seven states: Andhra Pradesh, Himachal Pradesh, Karnataka, Odisha, Uttar Pradesh, and Kerala. IHIP has been formally introduced in nine states so far.[130]

The National Health Stack (NHS) of NITI Aayog is a shared digital healthcare infrastructure used to oversee the Ayushman Bharat Scheme and other public healthcare programs. It consists of national electronic registries, a federated personal health records framework, and a national analytics platform. While the goal of the NHS may be to better implement welfare programs by utilizing patient data, there is the potential for misuse of this information. The Government's draft law, the Digital Information Security in Health Care Act (DISHA)of 2018[131], was introduced to remedy this. As a result of the Act, hospitals and clinics will be able to share personal health records digitally, and data owners will have "the right to privacy, confidentiality, and security of their digital data." It also provides health information exchanges to exchange electronic health records (EHRs) and the authority to regulate them.

The Health Data Management Policy 2020 (HDM) was published by the Ministry of Health and Family Welfare in August 2020. The HDM is the product of National Health Policy 2017 and the National Digital Health Blueprint (NDHB), intended to enable universal health coverage while protecting people's sensitive personal medical data. The NDHB proposed the National Digital Health Mission (NDHM), a fully-government organization with complete functional autonomy.

Over time, India has the opportunity to establish a legal framework that strikes the appropriate regulatory balance between advancing the benefits of public health surveillance while also protecting individuals' right to privacy. The question as to whether the newly proposed policies will coexist with the earlier draft bills is something that would be clarified only when these regulations are notified after proper considerations and deliberations.

[130]Annual report 2020-21, Department of Health & Family Welfare Ministry of Health & Family Welfare,https://main.mohfw.gov.in/sites/default/files/Annual%20Report%202020-21%20English.pdf , accessed on June 28, 2021

[131] Draft DISHA bill, https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf, accessed on June 28, 2021.

4.3. INADEQUACIES IN THE CURRENT HEALTH DATA PROTECTION REGIME IN INDIA

In India, hospitals are increasingly relying on electronic medical records (EMRs) to store patient data. In reality, the Clinical Establishments (Registration and Regulation) Act 2010, which governs the registration and continuing of clinical establishments, requires the keeping and provision of EHR for every patient, but it's the hard reality that the clinical establishment Act has not been properly implemented within the country. The adoption of clinical establishment act in private sector is very less and the regulatory overview prescribed under the act is ineffective and weak.

Section 43(a)[132] and section 72[133] of the Information Technology Act provide the broad framework for the protection of personal information in India. Section 43(a) along with the sensitive personal information rules – which lay down the compliances that need to be observed by an entity that collects or stores or otherwise deals with sensitive information such as passwords, financial information, health conditions, sexual orientation, medical records and biometric records – mandates corporates to take reasonable procedures to protect sensitive personal data or information and section 72 protects personal information from unlawful disclosure in a breach of contract. It is pertinent to note that section 43(a) applies only to a 'body corporate', defined as "a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities." Because the bulk of India's people cannot afford private healthcare, public medical services and hospitals are almost always utilised. If public hospitals or non-governmental organisations (NGOs) do not maintain reasonable security measures, there are few options for recourse, leaving a substantial amount of personal data unprotected.

The Electronic Health Record Standards provided by the Ministry of Health and Family Welfare is the current framework for governing EMRs in India (MoHFW). It establishes international technical, administrative, and physical standards for health-related data protection, but it's not legally enforceable. The EHR standards have a number of flaws, including an ambiguous scope of coverage, a lack of clearly defined timelines for accessing patient records, the failure to include unique identification information such as URLs and IP addresses as sensitive information, and an ambiguous definition of "personal health information" etc.

[132] Compensation for failure to protect data
[133] Penalty for breach of confidentiality and privacy

In India, there are no rules requiring hospitals to report security breaches. For example, the HIPAA mandates that a hospital disclose a breach that affects more than 500 patients[134]. As a result, there is no clear structure governing electronic medical records and how they are gathered and utilised, and there are no remedies for data breaches caused by public hospitals' negligence.

India should study the best practises for electronic health and medical records developed by countries with more developed governance systems. Given the highly sensitive nature of medical data and the devastating consequences of a breach on an individual's life, the government must expedite the proposed health data protection laws to cover all hospitals and other healthcare institutions ensuring that the regulator is quick to respond to cases of negligent security and misuse of personal information.

4.4. PROPOSED LEGISLATIONS FOR HEALTH DATA PROTECTION IN INDIA

4.4.1 DIGITAL INFORMATION SECURITY IN HEALTH CARE ACT (DISHA)

To ensure the confidentiality of "sensitive personal data," particularly health data, the Government is considering passing DISHA in addition to the recently introduced PDPB 2019, an amended version of the 2018 Bill. Both Bills are complementary to one another while remaining somewhat distinct. PDPB 2019 has a broader scope than DISHA, which covers all data types, including financial, biometric, and religious affiliation. On the other hand, DISHA is focused on regulating the processes associated with the collection, storage, transmission, and use of digital health data and ensuring the reliability, privacy, confidentiality, and security of digital health data. [135]

- NATIONAL AND STATE ELECTRONIC HEALTH AUTHORITIES

DISHA seeks to establish the National electronic Health Authority of India (NEHA)[136], State electronic Health Authorities (SEHA)[137], the National Executive Committee, and State Executive Committees to assist the NEHA and SEHA, as well as health information exchanges managed by the Chief Health Information Executive (CHIE), the data

[134] HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414
[135]Digital Information Security in Healthcare Act (DISHA), 2018, Preamble
[136]Digital Information Security in Healthcare Act (DISHA), 2018, §5
[137]Digital Information Security in Healthcare Act (DISHA), 2018, §7

controller[138]. The NEHA and SEHA shall have the same powers as a civil court under Section 26 of the DISHA, including summoning and examination of witnesses. As a result, DISHA recognizes the necessity of establishing specific bodies with jurisdiction over this type of dispute, seeing as how the courts are already overburdened with many cases.

However, DISHA provides for the following matters to be dealt with in Sessions Court [139]

- Theft of data.
- Obtaining health information about another person fraudulently or dishonestly that such person is not entitled to obtain.
- Where a significant breach of DISHA's digital health data occurs.

Additionally, DISHA categorizes the penalties for "breach" under Section 37 and "serious breach of digital health information" under Section 38 based on the data collector's criminal intent, i.e., prescribing penal consequences for the collector's intentional, fraudulent, or negligent breach of data. A severe violation of Section 38 carries a sentence of three to five years in prison or a fine of rupees five lakhs, provided that the acceptable amount may be paid in whole or in part to the victim of the violation at the Court's discretion. On the other hand, a "breach" shall result in damages to the owner of such digital health data.

- COMMERCIAL USE PROHIBITED

DISHA expressly prohibits commercial use of digital health data.[140] The disclosure to insurance companies, employers, human resource consultants, and pharmaceutical companies is explicitly prohibited. This requirement applies to clinical settings, and health information exchange The nature of digital health data is irrelevant; the prohibition applies regardless of whether the data is identifiable or anonymous.

- INTEROPERABILITY OF HEALTH DATA

One of the irregularities addressed in DISHA is the transmission or transfer of data from one clinical facility to another, referred to colloquially as interoperability of health data or portability of health data.[141]Transferring a patient's health data to other clinical establishments avoids duplication and saves time and money. As enabled by DISHA, this provision will promote the reuse of digital health data and may result in health practitioners

[138]Digital Information Security in Healthcare Act (DISHA), 2018, §21
[139]Digital Information Security in Healthcare Act (DISHA), 2018, §43(2)

[140]Digital Information Security in Healthcare Act (DISHA), §38(d)
[141]Jyotiranjan Mallick, *Digital information security in Healthcare Act: Its impact on m-health vis-à-vis Personal Data Protection Bill, 2019*, NLUJ LAW REVIEW, (Aug. 6th 2020), http://www.nlujlawreview.in/digital-information-security-in-healthcare-act-its-impact-on-m-health-vis-a-vis-personal-data-protection-bill-2019/

discontinuing the repetitive prescribing of the same tests, one of which is a lack of access to the patient's medical history.

Additionally, DISHA seeks to establish a centralized regulatory authority to secure sensitive health data exchange. It states that the Government shall ensure that health information exchanges transmit data with the consent of the data principal, i.e., that a patient is to be treated as the sole owner of digital data and that no other party, including any clinical establishment or other entity, has the right to store the data without the data owner's written consent.

DISHA includes the following enabling provisos to ensure the confidentiality of digital health data:

(1) The NEHA shall establish protocols for transmitting and receiving digital health data from and to other countries under Section 22(1)(e), as well as standards for physical, administrative, and technical measures to ensure privacy and confidentiality of digital health data transmission.

(2) A clinical establishment shall transmit encrypted data to a health information exchange.

4.4.2 KEY DIFFERENCES BETWEEN DISHA AND PERSONAL DATA PROTECTION BILL, 2019

PROVISION	DISHA	PDP BILL
Ownership	Patient (Clause3(j))	
Definition of Health Data	Includes information about the health status, health services, donation or examination of a body part, and details of clinical establishment accessed by the individual (Clause 3(e)).	Includes data about physical or mental health, includes records regarding the past, present, or future state of the health, data collected/associated in the course of registration for, or provision of health services (Clause3(21)).
Regulatory Body	National Electronic Health Authority (NeHA) (Clause 4).	Data Protection Authority of India (Clause 41).
Regulate Entities	Clinical establishments (Clause 212(b)), Health Information Exchanges	Data fiduciaries (Clauses2A(C), 4-11)), Data processors (Clause2A(C)).

	(Clause 19, 20), any entity with custody of health data (Clause22).	
Commercial Use	Not allowed (Clause 29 (5))	Allowed (Clause 4)
Interoperability Provisions	NeHA to prescribe standards (Clause 22)	Limited to the protection of privacy & right to data portability (Clause 19).
Usage of Data	Concise, restrictive	Expansive
Consent Requirement	Yes (Clauses 28, 29, 30, 33 & 44(2)	Yes (Clauses 7, 9, 11, 16, 20, 23, 34, 40, 50, 82, 94)

4.4.3 CONSENT IN GENERAL UNDER PDP BILL VS. DISHA'S STRICTER CONSENT PRINCIPLE

The similarities between DISHA and PDPB 2019 is that both Bills control and restrict health data, which is sensitive information about a data principle, and both are consent-based. The contrast between the Bills is that DISHA sets stricter regulations, requiring agreement from the data principal at each stage (i.e., generation, collection, storage, processing, transmission, access, and disclosure). It requires the data controller to acquire consent before processing or retaining the data in the future. DISHA places a priority on permission from the data subject. It vests the data owner with a variety of rights under Section 28, including the following:

(a) The right to the privacy, confidentiality, and security of collected or stored digital health data.

(b) The right to refuse or grant consent to the use, generation, or storage of data for specific purposes, as well as the right to revoke previously given consent.

(c) It grants the owner the right to know which entities or establishments access the data.

(d) The right to object to the transmission or disclosure of any sensitive health information that is likely to cause the owner harm or distress.

(e) The owner has the right to direct health data sharing with family members in a medical emergency, etc.

(f) The right not to be denied health services if the data subject refuses to consent to the collection, storage, transmission, and disclosure of their health data.

Section 29(3) of DISHA expressly prohibits the use of data for any purpose other than those for which consent has been obtained. Other instances, namely for public health purposes, in which digital health data may be used include the following:

(a) To aid in the advancement of health and clinical research.

(b) To increase awareness of and capacity for chronic disease detection, prevention, and management.

(c) To conduct and analyze public health research.

(d) To conduct scholarly research.

Provided that such data is de-identified or anonymized in the above-mentioned circumstances, i.e., the natural person cannot be identified from such data. Thus, no consent shall be required in the aforementioned four instances, as well as when a statutory or legal requirement is imposed under DISHA. The precise instances of statutory or legal requirements are not mentioned expressly or in specific terms in the current version. They thus are dependent on any orders, court decisions, or other laws. DISHA is supposed to take precedence over any other law relating to digital health data, but there is some ambiguity in this regard, as discussed later.

According to the DISHA Bill, there is a prohibition on the disclosure or transfer of data to pharmaceutical companies, even though one would assume that "ownership" would include the right to alienate data that has been acquired. [142]

Section 31 of DISHA states that while the individual whose data has been digitized retains absolute ownership, entities or clinical establishments may use the data in trust for the owner. The approach is more relaxed and straightforward under PDPB 2019. Consent of the data principal is required for data use. Still, it also contains provisions that allow for data use without the permission of the other party, i.e., data can be used in medical emergencies, to provide benefits to the data principal who is a State employee, to comply with court orders, to control law and order situations, and to grant any license granted by the State[143].

The other basis for proceeding without consent is for "reasonable purposes,"[144]which include the following:

- preventing and detecting illegal activity;
- defamation;

[142]Digital Information Security in Healthcare Act, 2018, §29(5)
[143]The Personal Data Protection Bill, 2019, §12
[144]The Personal Data Protection Bill, 2019, §14(2)

- acquisitions and mergers;
- (d) information and network security;
- credit assessment;
- debt collection;
- (g) the processing of personally identifiable information that is publicly available; and
- (h) search engine operation.

Thus, the instances of non-consent-based handling of personal data, including health data, are more prevalent under PDPB 2019 than under DISHA.

4.4.4 PDPB OR DISHA: WHICH WILL PREVAIL IN 2021

Both the PDPB 2019 and DISHA have overriding clauses that indicate that their respective laws take precedence over any other legislation in the case of a disagreement. Section 52 of DISHA[145]and Section 96 of the PDPB[146] are the applicable provisions. This has the downside of allowing for potential misunderstanding when a litigant or a party opts for DISHA over the PDPB 2019, which has stricter consent conditions and greater privacy responsibilities. This problem should be resolved either by amendment or by adding more explicit regulations to the individual Bills once they are adopted to ensure that a party cannot simply exploit this loophole.

One can argue that sector-specific regulation is always desirable since it takes into account the sector's dynamics. On the other hand, enacting such legislation would be impossible. Additionally, PDPB will need to be revised to reflect contemporary healthcare sector trends to assure its continued relevance.

Additionally, Section 55(5) of DISHA contains an enabling clause requiring the Government to conduct a complete assessment of all health-related legislation within one year of DISHA's implementation to guarantee compliance.

Thus, it looks as though two alternative methods are cooperating — one on subsuming DISHA into PDPB to safeguard digital health data; and the other on creating consistent provisions or eliminating inconsistent ones to the degree feasible to prevent conflict with DISHA. To avoid duplication of effort, it looks as though the Ministry of Health and Family Welfare (MoHFW) and the Ministry of Electronics and Information Technology (MeitY) are arguing whether to integrate the protective measures for digital health data into the PDPB 2019 or its revisions.[147]There are chances that the DISHA bill will be scrapped, and the new

[145]Digital Information Security in Healthcare Act, 2018, §52
[146]The Personal Data Protection Bill, 2019, §96
[147]See https://pib.gov.in/Pressreleaseshare.aspx?PRID=1578929 , accessed on 19th june,2021.

Health Data Management Policy will supersede the same. This can be ascertained through the upcoming development in Healthcare legal regime in India.

India, despite being the world's largest democracy, has yet to enact core data privacy principles. The Indian Government has consistently failed to safeguard the confidentiality of databases obtained via Aadhaar and other biometric identification systems. Recent data breaches have occurred in several cases. In a recent survey by Compritech's Global Survey[148], India was ranked third worst for data privacy. Countries are ranked according to data enforcement, biometrics, and other considerations. The worsening position on the Global Surveillance Index demands the immediate implementation of PDPB 2019 and other sector-specific legislation such as DISHA, continuously postponed.

4.4.5 NATIONAL DIGITAL HEALTH MISSION (NDHM)- HEALTH DATA MANAGEMENT POLICY (HDM)

The Draft Health Data Management Policy encompasses the institutions engaged in the NDHM and the partners/individuals that comprise the National Digital Health Ecosystem (NDHE). These include, but are not limited to, entities and individuals who have been issued an ID according to the Draft Policy, healthcare professionals, health care providers who collect, store, and transmit health data electronically in the course of conducting business, drug manufacturers, medical device manufacturers, insurers, research organizations, and governing bodies such as the MoHFW.[149]

The Health data management (HDM) Draft Policy's objectives include, but are not limited to, the establishment of a framework for the secure processing of personal and sensitive personal data about individuals who are members of the NDHE following all applicable laws, the establishment of a system of digital personal and medical health records that is easily accessible to individuals and health care providers and is purely voluntary.[150]

The Draft Policy proposes the establishment of a Health Identification Card. A data principal may request a free Health ID to participate in the NDHE ecosystem. Any processing of personal data necessary to create such an ID must comply with the Draft Policy. The Health ID may be produced following the NHA's specifications and authenticated using the data

[148]Shanthi S, India *Ranked Third Worst For Data Privacy In Global Surveillance Index,* INC42.com, (Oct. 17th 2019), https://inc42.com/buzz/india-ranked-third-worst-for-data-privacy-in-compritech-global-surveillance-index/ accessed on 15th July, 2021
[149]Health Data Management Policy, 2020, §2
[150]Health Data Management Policy, 2020,§3

principal's Aadhaar number or another form of identity authorized by the NHA. A data principle's data will be connected to their Health ID, and any data principal in possession of such a Health ID is considered the data principal. Similarly, a health practitioner may request a free Health Practitioner ID, which will be necessary to participate in the NDHE.[151]

The Draft Policy establishes several requirements for the acquisition and processing of personal and sensitive personal data. Personal data or sensitive personal data can be collected or used by data fiduciaries (similar to data controllers) only with the agreement of the data principal.[152] Additionally, the objectives for which personal data will be processed shall be limited to those stated by the NHA.[153]Further, data fiduciaries must follow specific standards, including openness, accountability, and reasonable security policies and processes. Additionally, a data fiduciary must enter into confidentiality and non-disclosure agreements with data processors that address data protection and privacy obligations. Data fiduciaries must comply with the International Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" and any other applicable standard.[154]

Any personal data handled by a data fiduciary may be shared with a health information user (HIU) in response to such HIU's request for personal data about the data principal, but only with the data principal's agreement.[155]These HIUs are authorized to seek access to a data principal's data with the data principal's approval. Data fiduciaries may make aggregated or anonymized data available for facilitating health and clinical research, academic research, archiving, statistical analysis, policy formulation, the development and promotion of diagnostic solutions, and such other purposes as the NHA may specify. Any person or entity is not authorized to publish, exhibit, or post publicly any personal data or sensitive personal data of a data principal.[156]

According to the Draft Policy, the governance structure for the NDHE shall be established by the NHA, which will lead the NDHM's implementation. Additionally, the governance structure will include the committees, authority, and officials essential to execute the NDHM at the national, state, and health facility levels. Additionally, the MoHFW and the Ministry of

[151] Health Data Management Policy, 2020, Chapter IV
[152]Health Data Management Policy, 2020, §9.1
[153]Health Data Management Policy, 2020, §9.2
[154]Health Data Management Policy, 2020, §27.1
[155]Health Data Management Policy, 2020, §28
[156]Health Data Management Policy, 2020, §31.1

Electronics and Information Technology will significantly assist the NHA on NDHM-related matters.[157]

4.4.6 PDP BILL AND HEALTH DATA MANAGEMENT POLICY

While the PDP Bill has not yet been finalized in the Parliament, the contents in the Draft Policy appear to be strongly influenced by it. This move raises whether this policy attempts to implement provisions of the Bill that should have passed review during Parliamentary consideration. As a result, certain discrepancies might result in a dispute with these statutes. For example, rules enacted under the PDP Bill, particularly those relating to how data principals' rights are enforced, were intended to be dealt with thereunder. Additionally, due to various legislations now including the same or similar meanings for specific terms, discrepancies in definitions may create implementation difficulties. Managing over a billion persons' vital health data in the way intended is logistically challenging and carries a slew of potential dangers of breach and abuse. While the Draft Policy is an ambitious aim, it should take into account these obstacles and concerns.

4.5. REGULATION OF ELECTRONIC HEALTH RECORD IN INDIA- COMPARATIVE ANALYSIS AND SUGGESTIONS

The regulatory environment for digital health in India is examined and compared to those in the United States of America, the United Kingdom, and Australia. The collection, reception, storage, and processing, as well as electronic transmission of healthcare data, are governed by the IT Data Protection Laws of 2011, a set of rules established by the Information Technology Act 2000 (IT Act 2008) and the Privacy and Right to Information Act 2005. India likewise established voluntary standards for electronic health records in 2013, which were later revised in 2016. The standards included specific recommendations about interoperability, clinical informatics standards, data ownership, privacy and security, and the different coding systems.

When it comes to healthcare data protection, different countries have their legislation; However, the primary intent of all these legislations is patient privacy; there exists a notable difference in how health data is regulated and protected. Countries like the USA have enacted sector-specific healthcare data protection laws. Countries like Australia have incorporated health data and its protection as part of their Privacy Act through amendment.

[157]Health Data Management Policy, 2020, §6

The Government of India envisions a national digital health ecosystem comprised of interoperable electronic health record systems. This can only be accomplished through the adoption of healthcare IT standards. The EHR Standards for India is one effective project that enables consistent standards in healthcare practices, regulations, and processes. Though these standards were a significant leap in the health data protection regime, these are not legally enforceable. And at the current junction where we have several data protection drafts pending before the parliament, we can't have a clear inference as to whether we will have sector-specific legislation like DISHA or whether the health care data protection will become a part of the Personal Data Protection Bill. We will have clarity about this in the coming years. Just like any other country Indian health data regulation framework also focuses on Data ownership, Data Access and Confidentiality, Disclosure of sensitive information, and preservation of electronic health records.

Also, when it comes to the storage and preservation of health data, the every nation faces cyber threats irrespective of its technological advancement. In the USA, according to HHS, between 2009 and 2013, the top causes of data breaches affecting 500 or more individuals were: improper disposal (5%), hacking/IT incident (6%), loss (11%), unauthorized access (20%), and theft (54%).[158]2016 saw a 320 percent increase in breaches affecting 500 or more individuals caused by hacking/IT incidents.108 Therefore, while technology-driven violations caused a significant portion of the attacks, almost all breaches were caused in some way by human error. This indicates changes in administrative practices may result in better data security.[159] Therefore in this fast-growing world of the internet, a solid health data protection framework is very necessary-This can be at the administrative and technical levels. Every country should have an adaptive and sound mechanism to copewith the inevitable cyber threats.

Framework and implementation of electronic health record policies also vary from one country to other. This is primarily connected to their healthcare system and health infrastructure. When it comes to a country like Canada, where the state sponsors 90% of the healthcare expenditure, it's easy to implement any new system with the cooperation of all stakeholders in the healthcare system. But when it comes to a country like ours where 65% of the health expenditure is borne by the patient (out-of-pocket expenditure), it's challenging for

[158]MARGARET AMATAYAKUL, HANDBOOK FOR HIPAA-HITECH SECURITY 84 (American Medical Association 2013). (Analyzing the data from U.S. DEP'T OF HEALTH & HUM. SERV., OCR, Breaches Affecting 500 or More Individuals (last visited Oct. 29, 2016).

[159]Kim Zetter, *Why Hospitals are the Perfect Targets for Ransomware*, WIRED (Mar. 30, 2016), https://www.wired.com/2016/03/ ransomware-why-hospitals-are-the-perfect-targets/

the government to implement the standards uniformly. We still don't have the exact number of unregistered doctors or clinics practicing medicine in rural India.

Another concern is how the system is managed; for example, in Australia, EHR is Regionally managed, joint (national & state) open emergency clinic subsidizing general open clinical protection program(Medicare). In India, Financing, provisions, and guidelines are brought by the central government, financing plans, and direct arrangement of services by the state governments.

Australia empowers patients to manage their own EHRs through a digital health evidence review. According to a survey of 50 nations, Australia and France are the only countries that allow patients to modify and update their health records. Australia manages the MyHealth site, which is used in various circumstances ranging from emergencies to routine illness and patient care, as well as health and wellbeing.

The most comprehensive standard in the present scenario appears to be the Data Protection Directive, which identifies the data protection principles that form national data protection laws among EU member states. The Data Protection Directive is also evidence of a robust regulatory framework that restricts the power of third parties, including government bodies, to collect SPD. It's to be noted that in the current global scenario, it is difficult to find out an EHR protection regime that is perfect in all sense

In the context of India, the rationale for the adoption of EHR is not convincing. According to the DISHA, the mission is to provide patient care and conduct research. A consent framework is set for data usage. According to the Act, private organizations are prohibited from commercializing health data; nevertheless, there are several situations in which the state may utilize health data. The National Digital Health Blueprint (NDHB), on the other hand, has a considerably broader scope for the use of health data. From health and well-being for everyone at all ages to Universal Health Coverage, this encompasses citizen-centric efficient and effective services, responsibility for performance, and the development of a holistic and comprehensive health ecosystem, among other things. The vast scope of the NDHM's responsibilities confers significant authority on the state, responsible for regulating and appropriate using the data collected for any of the objectives mentioned above. As a result, it is necessary to specify the goal of EHR adoption for the standards produced under the framework to be compatible with such clearly defined plans.

In India, it is doubtful that DISHA would be adopted in its current form. The National Digital health Blueprint(NDHB) framework envisions establishing a National Digital health Mission (NDHM) as the primary regulatory agency responsible for putting the blueprint into action. In addition, the framework iterates a five-year level action plan to fulfil the defined goals. "developing and maintaining the foundational digital health data and the infrastructure necessary for its exchange...promoting the adoption of open standards...creating a system of personal health records based on international standards," according to the report. The principles outlined in the NDHB do not adequately address telemedicine, consent withdrawal and the right to be forgotten, de-identification of data, and other related issues. Without a legislative mandate and financial backing, the private healthcare industry has insufficient incentives to implement the design.

Furthermore, the Patient Data Protection Bill (PDP Bill) of 2019 places the patient in control of their health data through a consent framework but does not refer to the patient as the data owner. Any legitimate commercial use of health data would be permitted under the PDP bill, provided that the patient agreed to such use. Nonetheless, the legislation has extensive exclusions, particularly allowing the state to use data without consent, including any actions taken to give help or services in the event of a disaster or a breakdown in public order.[160] One of the significant concerns with the PDP Bill is the state's ability to identify Sensitive Personal Data and enact rules in this area.

Since 2009, the United States' HITECH Act has enforced a phase-wise introduction of electronic health records (EHRs). They are still improvising and finetuning their system to adapt to the changing times. When it comes to India, EHR adoption is still in the rudimentary stage. Therefore, we must have a long-term vision and goal, considering the global measures adopted by different countries.

4.6. CONCLUSION

While the DISHA and HDM look promising, their implementation and enforcement have yet to be thoroughly tested, not to mention the Personal Data Protection Bill of 2019, which continues to be a cause of concern. There is a lack of coordination and uniformity across ministries, which might result in violations of sectoral legislation controlling health data and set India back in the race to create the much-desired 'culture of privacy,' which would be detrimental to India's international standing.

[160]Section 12 to 15 of the Personal Data Protection Bill.

5. CHAPTER 5: HEALTH INFORMATION AND RIGHT TO PRIVACY IN INDIA

5.1 INTRODUCTION

In India, currently, no particular regulations are governing the disclosure of medical records or records of treatment. According to the Indian Medical Council Regulations, however, every medical practitioner must respect the confidentiality of the physician-patient relationship.[161] In addition, while a physician who divulges personal information about their patients may face disciplinary action for professional misconduct[162], this duty does not apply to other individuals responsible for processing patient data,[163] whether they are employed by a governmental agency or by a corporation. Only under certain circumstances, such as a 'serious and recognized risk to a specific individual and community,' are physicians permitted to reveal patient information to public health authorities. [164]We have had recent development in the right to privacy, and which had triggered various products in the field of data protection in India

5.2 RIGHT TO PRIVACY IN INDIA

The term privacy has been described as the rightful claim of the individual to determine the extent to which he wishes to share himself with others and his control over time, place, and circumstances to communicate with others. It means his right to withdraw or participate as he sees fit. It also means the individual's right to control the dissemination of information about himself if it's his possession.[165]

[161]The Indian Medical Council (Professional Conduct, Etiquette and Ethic) Regulations, 2002, (102 of 1956). ('Medical Council Regulations').
[162]The Indian Medical Council (Professional Conduct, Etiquette and Ethic) Regulations, 2002, (102 of 1956), Chapter 8 (Disciplinary action may be taken against physicians for any offences committed in violation of the regulations).
[163]The Indian Medical Council (Professional Conduct, Etiquette and Ethic) Regulations, 2002, (102 of 1956), Rule 1.1 ('Character of Physician' covers only "Doctors with qualification of MBBS or MBBS with post-graduate degree/diploma or with equivalent qualification in any medical discipline" are covered under the Regulations).
[164]The Indian Medical Council (Professional Conduct, Etiquette and Ethic) Regulations, 2002, (102 of 1956), Rule 7.14.
[165]Edward Shils, *Privacy: Its Constitution and Vicissitudes*, 31 *L*aw and *C*ontemporary *P*roblems 281-306 (Spring 1966)

5.3 CONCEPT OF RIGHT TO PRIVACY-POSITION BEFORE PUTTUSAMY JUDGEMENT[166]

In contrast to the tendency in the United Kingdom and the United States, the Indian judiciary had recognized the right to privacy as an exception to the general norm that allows public authorities to interfere in an individual's private life. The Supreme Court had made it clear on several occasions that the right to privacy was not inalienable.[167] Instead, the Court has decided to use a case-by-case approach in interpreting the right to personal privacy.[168]Indian courts have granted the hospital permission to inform a patient's potential spouse of his HIV condition.[169] The public welfare argument, which states that the negligent transmission of an infectious illness constitutes an offense against public safety, has been used as the basis for disclosure in such instances.[170] Compared to the European Court of Human Rights' rights-centric approach in me v. Finland,[171] Indian courts construed individual autonomy solely regarding whether or not an interface with public interest existed; this approach places a strong emphasis on whether or not an interface with public interest occurs.

To resolve the conflict between an individual's "right to be left alone" and the "greater benefit" of the community, the Court has tended toward favouring the public good above individual privacy in recent years. In *Sharda v. Dharmpal*, a husband sought a divorce because his wife had a mental illness. As part of the investigation, the wife was obliged to participate in a medical examination. Having been forced to do so without her agreement, she argued that this would be a violation of her liberty. Aside from declaring that there is no absolute right to privacy, the Court found that a lack of such information would make it difficult to conclude the circumstances of this case.[172]

5.4 DEVELOPMENT OF RIGHT TO PRIVACY IN INDIA

The Supreme Court stated in *Gobind v. State of M.P*[173]held that the right to privacy encompasses and protects the intimate intimacies of the home, family marriage, maternity, reproduction, and child-rearing, subject to "compelling State interest."

---

[166]Justice K.S.Puttaswamy (Rtd) v. Union Of India (2017) 10 SCC 1.
[167]Sharda v. Dharmpal, AIR 2003 SC 3450.
[168]Govind v. State of Madhya Pradesh, AIR 1975 SC 1378.
[169]Yepthomi v. Apollo Hospital Enterprises Ltd., AIR 1999 SC 495; Mr. 'X' v Hospital 'Z', (1998) 8 SCC 296.
[170]Indian Penal Code 1860, §269, No. 45, Acts of Parliament, India (1860). (Non-disclosure of HIV+ status may be considered an offence, 'Negligent act likely to spread infection of disease dangerous to life').
[171]I v. Finland, Application No. 20511/03: 2008 ECHR 623 (The ECHR stated (upholding the Court's previous decision in Z v. Finland, (1988) 25 EHRR 371) that the protection of personal data, in particular 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 European Convention on Human Rights. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention).
[172]Sharda v. Dharmpal, AIR 2003 SC 3450.
[173]Gobind v. State of M.P (1975) 2 SCC 148.

In *People's Union for Civil Liberties (PUCL) v. Union of India*[174] held that, while considering the question of telephone tapping, the Supreme Court extended the right to privacy to communications and concluded that telephone tapping is a severe breach of an individual's privacy.

In *Selvi v. the State of Karnataka*,[175] the Supreme Court recognized the distinction between bodily/physical and mental privacy. It held that subjecting a person without his consent to techniques such as narco-analysis, polygraph examination, and brain electrical activation profile (BEAP) test violates the subject's mental privacy.

In *Unique Identification Authority of India v. Central Bureau of Investigation*[176], the Central Bureau of Investigation sought access to the Unique Identification Authority of India's database to investigate a criminal offense. In an interim decision, the Supreme Court decided that the Unique Identification Authority of India should not transfer any biometric information about an individual who has been assigned an Aadhaar number to another agency without the individual's written authorization.

Finally, in *S. Puttaswamy v. Union of India*,[177] the Court asked if the Constitution protects the right to privacy. If so, where does it come from, given that the Indian Constitution makes no explicit provision for confidentiality? Finally, a Supreme Court Bench comprised of nine judges resolved the case, concluding that the Indian Constitution contains a fundamental right to privacy.

The ruling reversed *M.P. Sharma v. Satish Chandra*[178] and *Kharak Singh v. State of Uttar Pradesh*[179]. In M.P. Sharma v. Satish Chandra[180], a Supreme Court of India eight-judge Bench decided that the Indian Constitution does not protect the right of privacy.

In *Kharak Singh v. State of Uttar Pradesh*[181], the majority opinion concluded that the Constitution does not provide a right. However, the basis for the right to as a fundamental right was set by the minority judgment rendered in this case by K. Subbarao and K.C. Shah.

[174]People's Union for Civil Liberties (PUCL) v. Union of India (1997) 1 SCC 301.
[175]Selvi v. State of Karnataka (2010) 7 SCC 263.
[176]Unique Identification Authority of India v. Central Bureau of Investigation (2017) 7 SCC 157.
[177]. Puttaswamy v. Union of India (2017) 10 SCC 1, 509-510.
[178]M.P. Sharma v. Satish Chandra 1954 SCR 1077.
[179]Kharak Singh v. State of Uttar Pradesh (1964) 1 SCR 332.
[180]M.P. Sharma v. Satish Chandra 1954 SCR 1077.
[181]Kharak Singh v. State of Uttar Pradesh (1964) 1 SCR 332.

They recognized the right to privacy as a fundamental right under the Indian Constitution's Articles 21 and 19(1) (d).

The minority decision, taken in conjunction with the judgment in *K.S. Puttaswamy v. Union of India*[182] is noteworthy because it established the "right to privacy" as a fundamental right in and of itself.

5.5 PUTTUSAMY JUDGEMENT

Since its beginning, THE CONCEPT OF 'PRIVACY' has been the subject of controversy, discussion, and deliberation—however, the Supreme Court's recent decision in Justice K.S. Puttaswamy (Retd) v. Union of India[183] elevated the concept of privacy in India since it addressed issues about the Aadhaar database. Aadhaar is a database that contains information about citizens' intrinsic characteristics, including their biometric data. This establishes a provision for informational privacy or the privacy of a person's information.[184] The demand of Aadhaar for access to social welfare systems was considered to violate an individual's right to privacy. Since Aadhaar contains biometric data and is linked to bank accounts, permanent account numbers (PANs), and other information, there is a strong possibility that the data collected and connected through Aadhaar will be misused, thereby jeopardizing citizens framework of interests regarding privacy.

Puttaswamy verdict reaffirmed the notion of proportionality by dividing it into four subparts:

(a) A restriction on the right must be justified.

(a) It must be a suitable means for accomplishing this objective.

(c) There must be no less restrictive option that is similarly effective.

(d) The measure shall not impose an undue burden on the right holder.

In *Puttasamy v. UOI*[185], Justice DY Chandrachud has enumerated that-

> "*Privacy is the constitutional core of human dignity. Privacy has both a normative and descriptive function. Privacy sub-serves those eternal values upon which the guarantees of life, liberty, and freedom are founded at a normative level. At a descriptive level, privacy postulates a bundle of entitlements and interests which lie at the foundation of ordered liberty;.*"

[182]K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
[183]Justice K.S. Puttaswamy (Retd) v. Union of India (2017) 10 SCC 1.
[184]R.Venkata Rao, Subha Rao (eds), *A Public Disclosure on Privacy – An Analysis of Justice K.S. Puttaswamy v. UOI*, 1 NLSIU, Bangalore (2018).
[185]Justice K.S. Puttaswamy (Retd) v. Union of India (2017) 10 SCC 1.

In *Puttasamy v. UOI*[186], Justice Sanjay Kishan Kaul has enumerated that-

> "*Such a right cannot be exercised where the information/ data is necessary, for exercising the right of freedom of expression and information, for compliance with legal obligations, for the performance of a task carried out in public interest, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defense of legal claims. Such justifications would be valid in all cases of breach of privacy, including breaches of data privacy*."

This seminal decision dramatically altered the way the Government viewed the privacy of its citizens, both in practice and in law. It demands governments implement structural reforms, increase transparency and accountability in commissioning and executing surveillance projects, and establish a system for judicial review of surveillance requests. It requires governments to exercise extreme caution and sensitivity in their care of citizen's personal information. It entails enacting a game-changing, rights-based data protection law that holds accountable all-powerful entities that handle individuals' data (data controllers), including the state.

In was the aftermath of this judgment, the Government created an expert group on data protection, chaired by Justice B N SriKrishna, in July 2018 and submitted its findings along with a draught Data Protection Bill. The Report made numerous proposals to enhance India's privacy laws. It proposed data processing and collection restrictions, the establishment of a Data Protection Authority, the right to be forgotten, data localization, and explicit consent requirements for sensitive personal data, among other things. However, the data protection bill is pending and so has not been implemented.

The concept of privacy and how courts interpret privacy have gone through an unprecedented change after this judgment. It has to be kept private regarding health information, and patient privacy should be maintained at any cost.

A rights-based data protection law is urgently needed, as is comprehensive surveillance reform that prohibits mass surveillance and establishes a judicial oversight mechanism for targeted management, as well as recognition of the principle that the state should be a model data controller when it comes to dealing with citizens' personal information. To fulfil its full promise, the privacy judgment must progress beyond impassioned dissents to complex,

[186]Justice K.S. Puttaswamy (Retd) v. Union of India (2017) 10 SCC 1.

enforceable decisions that restrain the political executive within clearly defined, constrained constitutional boundaries.

With a growing emphasis on digital health, data exchange and potential privacy breaches are significant concerns. Health information technology is one of the most private and secure sectors. With rising literacy rates and more access to knowledge via the internet, patients become more conscientious about handling their health records.

It is critical to standardize privacy and security rules and methods for managing electronic health records in such circumstances. Policies and procedures appropriate to paper-based health records would apply but would be insufficient for EHRs. It makes sense to advocate technology for process and policy management and technological standards for digital health record security.

5.6 RIGHT TO PRIVACY AND RIGHT TO INFORMATION

The right to privacy and the right to information are necessary human rights in the modern-day information society. For the most part, these two rights complement one another in making governments accountable to their constituents. However, when a request for access to personal information stored by government agencies is made, a contradiction between these rights may arise. States must create methods to identify critical concerns to avoid disputes and balance the rights where they overlap.

To enhance transparency and accountability in all public authorities' operations and enable individuals to obtain access to information under their control, the Government of India enacted an Act titled "The Right to Information Act, 2005" (RTI Act), which took effect on 15.6.2005. The Right To Information Act, 2005 (RTI Act) is intended to provide for the establishment of a practical regime for citizens to secure access to information under the control of public authorities to promote transparency and accountability in the functioning of all public authorities, the establishment of a central information commission and a state information commission has helped the same.

Sec. 4 of the RTI Act makes it a duty of public authorities to maintain records for easy access and publish within 120 days the name of the particular officers. They should give the information and regarding the framing of the rules, regulations, etc. Subsection (3) of sec. 4 states that for the performance of subsection (1), all information shall be disseminated widely and in such form and manner, which is easily accessible to the public.

While practicing medicine, a Registered Medical Practitioner (RMP) may encounter both medical and medico-legal issues. In the first scenario, the patient provides their health

information through a history, physical examination, and laboratory tests. In the latter scenario, such exercise is conducted by RMP in response to a request by the police or a court acting as a competent authority to order medico-legal examinations with or without permission.

The Indian Medical Council (Professional Conduct, Etiquette, and Ethics), Regulations, 2002 states that "Confidences concerning an individual's or domestic life entrusted to a physician, as well as defects in the deposition or character of patients observed during medical attendances, should never be revealed unless required by law."[187]

The same attitude of "Professional Secrecy" is mirrored in numerous sections of the Medical Termination of Pregnancy Act 1975, requiring all records about terminated women to be kept secret / confidential.[188]

In medico-legal cases, where the accused or his legal representative may request any information about the case, and according to Section 6 (2) of the RTI Act, "an applicant requesting information shall not be required to provide any reasons for requesting the information or any other personal information except those necessary for contacting him." Though the decision to consider such petitions must be made by the "State Public Information Officer" or his subordinate, the Forensic community should be aware of the following pertinent sections:

Notwithstanding everything else in this Act, no citizen will be obligated to provide,

- Information that has been expressly prohibited from publication by a court of law or administrative body or whose revelation would constitute contempt of Court.
- Information that might obstruct the investigation, apprehending, or prosecuting of criminals. [189]

The Right to Information Act, 2005, has inherent tensions between opposing rights, such as the right to privacy, autonomy, and public interest, particularly about the medical profession. Numerous situations directly conflict with RTI, such as medical reports, post-mortem reports, and medical records. Numerous such cases are appealed to appellate authorities, namely the Central Appellate Authority appointed under the Central Information Commission and various courts, including High Courts and the Supreme Court of India. Numerous

[187]The Indian Medical Council (Professional Conduct, Etiquette, and Ethics), Regulations, 2002, §2.2
[188]Medical Termination of Pregnancy Act, 1971, No. 34, Statement of object and reasons, Acts of Parliament, India (1971).
[189]Right to Information Act, 2005, No.22, §8(1), Acts of Parliament, India, (2005).

contradicting CIC and court decisions in these cases further muddled the subject of RTI and the medical profession.

According to the Court of Appeal in *Shri G.R. Rawal v. Director General of Income Tax (Investigation),*[190]the scope of Section 8(1)(j) of the Right to Information ('RTI') Act, 2005, which prohibits the sharing of 'personal information in response to an application, was examined. On the other hand, the Central Information Commission ruled in this instance that the exclusionary rule would not apply in cases when the greater public interest warrants publication of the information in question. Following a 2007 judgment of the Bombay High Court, which permitted revelation of a prisoner's medical status in answer to an RTI application[191], it was further indicated that a determination of whether or not a disclosure was acceptable would be made on a case-by-case basis. However, while there may be exceptional circumstances that allow disclosure in the public interest in some situations, the judicial tendency seen in these cases has resulted in a steady erosion of the values of personal liberty and autonomy, as well as the right to remain silent. Without a doubt, the Supreme Court's use of the case-by-case approach to defining privacy did not afford the kinds of safeguards available under a robust data protection framework that respects the individual's autonomy.

A further point of contention is that Indian courts have ruled that data from a publicly available record cannot be safeguarded under the right to privacy.[192]The fact that public records might include hospital records, jail records, and any other information acquired by a state entity may have the effect of circumventing any authorization requirements for obtaining patient data that is already stored in public records as a result of this judgment. To ensure that information in the hands of the state is protected, comprehensive data protection legislation must be established and enforced.

5.7 RIGHTTO HEALTH AND PRIVACY– CHANGING DIMENSIONS

You may have noticed that the Government has been promoting data as the panacea for all problems over the last few years. Because if obtaining sufficient data would automatically resolve all the issues plaguing our country for years and generations. However, this is not the case. The system indicates that a substantial amount of data is being collected, accumulated, analysed, and put to various uses. There are multiple players in this ecosystem, including

[190]No. CIC/AT/A/2007/00490 (decided by Central Information Commission on March 5, 2008) ('G.R. Rawal').
[191]Mr. Surupsingh Naik v. State of Maharashtra through Additional Secretary, General Administration Deptt., AIR 2007 Bom 121.
[192]Mr `X' v. Hospital 'Z', (1998) 8 SCC 296.

doctors, health workers, and nurses (who potentially do not know the data they are collecting and analysing; putting it into a system they do not know how to operate).

Because of the porous interface between the right to privacy and medical treatment, personal health data protection is a top priority for many people. A patient's personal health information is entered and stored online at the point of care throughout their lifetime, from the time of their first admission or attendance at the hospital to the time of their final laboratory tests. The information is readily available and accessible to all healthcare providers in charge of the patient; however, the scope and nature of the data collection are unprecedented in their scope and nature. To mention the risks that can arise when this information is combined with that of other sources, such as pharmaceutical companies, leading to manipulative marketing, data breaches, discriminatory profiling, and the re-selling of personal information instead of online trading activities are all possible consequences.[193]

The right to privacy is subject to reasonable restrictions for prevention of crime, disorder, protection of health or morals, or protection of rights and freedom of others. There is a conflict between two derived rights, which advance public morality and public interest prevail.

In the case of electronic health records (EHRs), the Right to Health (RTH) and the Right to Privacy (RTP) are not always in conflict. Electronic health records (EHRs) have the potential to strengthen the right to privacy by giving patients a greater sense of control over the management of their health. Article 12 of the International Covenant on Social and Economic Rights requires states to prevent or control the spread of disease through techniques such as epidemiological data research, which can be improved through the use of electronic health records.

At the same time, there are instances where the right to health and privacy may be at odds with one another. For example, when data is collected for research purposes, it is still considered personal information even if it is anonymized and de-identified. While research is necessary for determining the causes of diseases, developing preventive measures, and discovering cures, collecting data for these purposes may violate the right to privacy. However, the irony is that there is an ethical duty of rescue that applies in this situation, which means that people are required to consent to and allow their data to be used when there

[193]Kathryn C. Montgomery and others, *Health Wearable Devices in the Big Data Era : Ensuring Privacy, Security, And Consumer Protection*, CDD Report, 2017, DEMOCRATIC MEDIA, https : //www.democraticmedia.org/sites/default/files/field/public/2016/aucdd_wearablesreport_final121516.pdf(last accessed 2 June 2021).

is a minimal risk associated with the use of the data. Our data protection bill also contains a provision that permits research on anonymized data to be conducted without obtaining consent; however, in this case, the exemption is granted on the basis that obtaining consent is impractical and there is a reasonable public interest. In allowing such research."

The debate concerning human guilt in the COVID-19 outbreak has only recently begun and is likely to dominate global discourse and governmental issues for some time to come.[194]India's primary objective is to eliminate Covid-19 through prevention, mitigation, and control. Both the Central and State Governments have taken several measures to accomplish this goal, and they are cooperating closely.

In light of the current crisis, several states in India have created an online database of people afflicted with this disease or confined in their homes or government-run facilities. Some jurisdictions have even gone so far as to plaster notices outside the homes of those who have been quarantined, most likely in the hope of alerting other residents in the area.

The entire issue of the State containing the pandemic through various methods will confront an impediment in the shape of individual privacy or be pushed aside in favor of a broader public interest during the pandemic.

However, unlike other fundamental rights protected by the Indian Constitution, the right to privacy is not an absolute fundamental right and can thus be reduced by the State. Even in the Aadhaar case, three criteria were established to determine the legitimacy of an Act violating any right: first, the activity must be authorized by law (lawfulness). Second, the activity must be necessary for the achievement of a certain objective (need). Third, the activity (invading privacy) must be appropriate to the need for it. [195]

Any state that has published the names and addresses of persons who have COVID 19 and has pasted the so-called notice outside the homes of those who have been quarantined appears to be breaching these individuals' right to privacy.[196] The States' actions will raise a constitutional question about whether all of these policies can withstand judicial scrutiny under the Puttaswamy Case.

---

[194] Wendy K. Mariner, *Reconsidering Constitutional Protection for Health Information Privacy*, 18(3) University of Pennsylvania Journal of Constitutional Law, 975, 2016

[195]Vikram Koppikar, *Covid-19 : Data Privacy in these Testing Times,* MONEY CONTROL: INDIA, 27 June 2020, https : //www.moneycontrol.com/news/economy/policy/covid-19-data-privacy-in-these-testing-times-5120201.html, (last accessed 27June 2021).

[196]Soutik Banerjee and others, *Privacy in Times of Corona : Problems with Publication of Personal Data of COVID-19 Victims*, LIVE LAW, 26 March 2020, https : //www.livelaw.in/columns/privacy-in-times-of-corona-154360?infinitescroll=1 (last accessed 27 June 2021)

The Central Government launched the 'Arogya Setu' smartphone app, which would notify users if they encounter a COVID-19 positive patient and what precautions they should take. However, cyber security experts highlighted concerns that 'Arogya Setu' may infringe on a COVID-19 positive patient's right to privacy.[197]According to the app's privacy statement, it collects personal data from users. It discloses such health data to the Government with the relevant details for 'carrying out medical and administrative interventions necessary in connection with COVID-19.[198]Additionally, the app is more intrusive than the browser. It captures many and sensitive personal data, posing a privacy concern. However, it is equally reasonable to assert that during the outbreak of any epidemic disease, the Central Government has the authority to take any 'necessary steps' to prevent the spread of the disease in the public good. [199]To satisfy the proportionality criteria, any action was taken by the Central or State governments that breaches the Fundamental Rights of its inhabitants must not be 'excessive.' That is, no existing measure should be equally efficient with a reduced degree of incursion.[200]*Puttaswamy v. UOI* [201] refers to this period as the 'necessity stage.' Certain governments have implemented a policy of using indelible ink to stamp individuals who have been tested positive or who have been quarantined.

States' actions may have a rational purpose (i.e., to prevent and control the spread of Covid-19 by minimizing contact of people and following social distancing). Given that the State's primary goal is to prevent people infected with the virus from coming into contact with other people, it would appear that physically stamping and identifying dwellings accomplishes this goal and that publishing a database of sufferers is entirely unnecessary.

There are several issues with posting an online database, including the personal health information of COVID-19 patients. Without a specific data protection law in the country, which appears to be a continuous violation of the Supreme Court's order upholding the constitutionality of the Aadhaar Act[202], the personal data of these people is being made public without their consent and is therefore vulnerable to misuse and abuse. This pandemic has also

[197]ManaviKapur, *The Corona Virus App Narendra Modi Endorsed is a Privacy Disaster*, QUARTZ INDIA, 15 June 2020, https : //qz.com/india/1838063/modis-aarogya-setu-coronavirus-app-for-india-a-privacy-disaster/, (last accessed 27 June 2021).

[198]KashishAneja and Nikhil Pratap, *Implement Arogya Setu but Only through Law*, THE HINDU, 21 June 2020, https : //www.thehindu.com/opinion/op-ed/implement-aarogya-setu-but-only-through-law/article31391708.ece, (last accessed 27 June 2021).

[199]Epidemic Diseases Act 1897, No.3, Acts of Parliament, India (1897).

[200]V.N. SHUKLA, CONSTITUTION OF INDIA 754 (11th edn, Eastern Book Company 2008).

[201]Writ Petition (Civil) No 494 of 2012.

[202]*supra* at 1.

increased xenophobia, bigotry, and racial violence, with hate crimes and mob lynching allegations.

We live in an era in which once material is uploaded to the internet for public consumption, it can never be deleted. Personal information about persons quarantined for Covid-19 will survive the current infection and will stay publicly available in perpetuity. Then what happens to these humans' rights to be forgotten on the internet and their identities once reduced to a stigmatized database entry? As we have seen throughout history, stigma frequently outweighs rationality and sagacity and has a life of its own.

It is primarily due to states' propensity to view civil freedoms as critical during times of crisis, conflict, or disaster. Some argue that it is the moral thing to do, and arguably, the Constitution recognizes this by including Articles 352- 360[203], which depict a drastically altered society in times of emergency. Nonetheless, in dealing with COVID-19, we must remember that civil liberties and rights are not the Executive's exclusive domain. The real litmus test for any democratic government is its ability to navigate this issue with the fewest possible deviations.

5.8 INDIAN PRIVACY REGULATIONS AND HEALTH INFORMATION PRIVACY

Privacy of information is a component of the right to privacy. In an information era, privacy threats might come from the state and non-state actors. The Court emphasizes to the Union Government the importance of examining and implementing a comprehensive data protection policy. Establishing such a system necessitates a careful and delicate balancing between individual interests and justifiable state considerations.

5.8.1 HEALTH PRIVACY PROVISIONS IN INDIAN LEGISLATIONS

Other than the draft regulations like PDP Bill and DISHA bill, which we have already discussed, patient privacy is protected by other separate Acts for specific purposes, the most significant of which are as follows:

a) Medical Termination of Pregnancy Act, 1971

A woman has the right to an abortion within her physical privacy, but autonomy and decision-making are not permitted. This is even prohibited for patients and their families

[203]Constitution of India, Part XVIII, Emergency Provisions

during the baby's sex determination. Written permission from the patient is required to facilitate an abortion. Such information may be disclosed exclusively to the State's Chief Medical Officer. Written authorization means that the patient is informed of all available alternatives, dangers, and post-abortion care and counseled about the procedure. The latest amendment[204] to the Act enhances the upper gestation limit from 20 to 24 weeks for special categories of women, which will be defined in the amendments to the MTP Rules and would include survivors of rape, victims of incest, and other vulnerable women (like differently-abled women, minors), etc.[205]The new amendment also specifies that the "name and other particulars of a woman whose pregnancy has been terminated shall not be revealed," except to a person authorized in any law that is currently in force[206].

b) *Mental Health Care Act, 2017*

The legislation restricts the nature and scope of information collection by relevant agencies and the acquisition of data and its use or dissemination. A doctor's medical certificate contains information about the nature and severity of the mental illness. Additionally, no inspecting officer is permitted to disclose a patient's records under this statute. Every person with mental illness shall be protected from cruel, inhuman, or degrading treatment in any mental health establishment and shall have the right to privacy.[207]

c) Pre-Conception and Pre-Natal Diagnostic Techniques (PCPNDT) Act, 1994

This Act was formed in the public interest for the prevention of female feticide. Pre-natal diagnostic testing is required for a mother to follow to determine her consent age, abortion history, and family history. A woman must disclose any family history of mental retardation or physical abnormalities to pass this exam. The Act places a premium on privacy and secrecy regarding genetic information sharing. The 2002 amendment to the Act mandates that all records, charts, forms, reports, consent letters, and other details shall be preserved for two years.[208]It also says that the appropriate authority has the power to search and seize if they have adequate reason to believe that the offense under the Act is committed.[209]

[204]The Medical Termination of Pregnancy Amendment Act, 2021
[205]Section 3(2)(b) of The Medical Termination of Pregnancy Amendment Act, 2021
[206]Section 5 A of The Medical Termination of Pregnancy Amendment Act, 2021
[207]Section 20 (2) (d) of the Mental Healthcare Act, 2017
[208]Section 29, The Pre-Natal Diagnostic Techniques (Regulation And Prevention Of Misuse) Amendment Act, 2002
[209] Section 30, The Pre-Natal Diagnostic Techniques (Regulation And Prevention Of Misuse) Amendment Act, 2002

d) Insurance Regulatory and Development Authority (Third Party Administrators), Health Services Regulations, 2001

The IRDA has prohibited insurance recommendation businesses from sharing their clients' information without their prior consent. Third-party Administrators are obligated to protect the confidentiality of data gathered on behalf of the insurance company. Third-party Administratorsarerequiredtokeepthisinformationfornotlessthanthreeyears.There is an exemption where a Third-party Administrator is requested to give pertinent information to a Court of Law/Tribunal, the Government, or any other Authority in connection with any inquiry conducted or planned to be undertaken against an insurance company.

e) Indian Medical Council Regulations, 2002

The Medical Council of India (MCI) has established a professional standard for medical practice in its 2002 Code of Ethics Regulations. This Act prohibits the collection of overly personal information from performing any of the procedures mentioned above. Physicians are required to protect patient confidentiality throughout the process.

This information includes any individual and domestic details. The Act may be waived if there is a risk to a specific person or community due to a disease.

f) National Ethical Guidelines for Biomedical and Health Research involving Human Participants, 2017[210]

The guideline establishes a restriction on the amount of information gathered and how it can be used. The privacy information contains the option to prohibit collecting their biological samples, the possibility of present and future uses of the biological samples obtained, and the danger of discovering any sensitive information. The identity of human subjects of research records should be kept confidential and should not be disclosed without valid scientific and legal reasons.[211] The guideline has listed out a set of obligations upon the researcher that he/she should maintain while researching human subjects to maintain the subjects' privacy

[210]National Ethical Guidelines for Biomedical and Health Research involving Human Participants, 2017, https://main.icmr.nic.in/sites/default/files/guidelines/ICMR_Ethical_Guidelines_2017.pdf, accessed on July, 28,2021

[211]Statement of General Principles, National Ethical Guidelines for Biomedical and Health Research involving Human Participants, 2017.

and confidentiality.[212] The guideline also speaks about the privacy and confidentiality that must be maintained while conducting social and behavioural science research.[213]

5.9 CONCLUSION

In the context of healthcare, the right to privacy of the patient is essential. While India's lead in the race toward a privacy culture continues to grow, the country is also capable of slipping to a distant second position in a short period. Although the gathering of consumer health data is increasing significantly, nothing is known about the extent to which this data is shared with other parties, which is especially important when confronted with an unseen enemy in the shape of the COVID-19 virus.

It's evident that the increased monitoring to handle the present healthcare crisis runs the risk of becoming the 'new normal,' putting people's privacy at risk. As part of its responsibility and democracy, a state will only collect the information necessary to achieve specific objectives and erase that information after it has been completed.

[212]Rule 2.3, Privacy and Confidentiality, National Ethical Guidelines for Biomedical and Health Research involving Human Participants, 2017.

[213]Rule 9.2.7, Privacy and Confidentiality, National Ethical Guidelines for Biomedical and Health Research involving Human Participants, 2017.

6. CHAPTER 6: CONCLUSION AND SUGGESTIONS

6.1 INTRODUCTION

Health records are vital to patients, health providers (including hospital systems and physicians), and health insurers. Patient data needs to be managed under a mandate of control, privacy, and accountability.[214]

In this fast-paced economy, the law continues to lag behind commerce, particularly in the area of privacy and data security. Healthtech companies collect a massive amount of sensitive personal data, mainly through self-monitoring health gadgets and mobile applications. Healthtech is one of the evolving business areas and has attracted contributions from the top venture capitalists in the recent past. Most creative and disruptive new-age industries move quickly, break things and then seek permission afterward. This is no exception in the case of healthcare.

India hopes to establish a set of standards that will aid in the achievement of interoperability and the increased use of electronic health records (EHRs). It is critical to emphasize that the drive for EHR adoption occurs in the absence of any data privacy or health data protection legislation. At present, we have legislations like DISHA and HDM, which are still pending before the parliament. It must be high time to have a data protection regime, primarily focusing on the healthcare sector.

The problem of a diverse population served by a fragmented healthcare network in India will make the interoperability of EHRs impossible without a proper regulatory framework. Additionally, it is critical to highlight that a purely legal mandate without a practical roadmap for acceptance and usage will be difficult to execute in a country like ours. A thorough debate of the exercise's aim, backed up by scientific investigation via regulatory effect assessments. Strengthening the current regulatory framework for healthcare is a necessary prerequisite for developing a legislative foundation.

6.2 CONCLUSION

Replacing the traditional offline record keeping system is not an easy task, especially when it comes to a country like India. But the digital revolution is inevitable even in the healthcare sector. Though there are rural areas in India where the internet has not crept in, this is the right time for the significant shift to EHRs. There need to be a lot of fine tuning before we

[214]Sarah J. Tomlinson Donna K. Hammakernna Yilmaz C. Kaymak,5th Eds, HEALTH RECORDS AND THE LAW, (Jones & Bartlett Learning LLC, 2019)

have a robust system established. EHR, if implemented with diligence, can effectively replace traditional health record keeping.

India doesn’t even have a sound data protection regime till date. The EHR standards of 2016 can't be considered an effective means to regulate a new system like EHR, which deals with sensitive personal data. But we have many sector-specific and general data protection regulations in the pipeline, which could be implemented in the near future. Proper implementation of the above-discussed draft legislation can protect the Indian healthcare regime. Currently, we only have very few legislations like the PNDT Act, which has express provisions for the protection of patient privacy. But implementing the draft legislations like DISHA or HDM could change the scenario, as these are sector-specific legislations focusing more on the patient's privacy.

In India, the healthcare sector is very unorganized, and we have many small and huge private players who dominate the market. There is an unavoidable necessity to incorporate protections that govern the safety of patient data once it is accessed by third parties, like insurance companies. The identification system, which assigns unique numbers to an individual's data and restricts access to that number or series of digits, may be implemented into the Indian scenario, simplifying the administrative process and boosting its efficacy. Individuals would retain their anonymity while transacting with specialized healthcare organizations.If we can bring in a standardized EHR regime applicable to all, it definitely can revolutionize the Indian healthcare sector.

It is critical to handle privacy issues about the international movement of personal data in the most feasible manner. This would need international cooperation and coordination to resolve privacy issues, including creating explicit requirements and consistent minimum criteria for international data transfer agreements. This interchange of ideas and multilateral debate would result in more effective techniques for enforcing privacy laws in domestic jurisdictions.Currently, we don't have any binding international agreements on EHR. But having an internationally binding agreement that could standardize EHR across the globe could enable the easy cross-border transfer of health data, thereby increasing healthcare accessibility.

As of now, we have a fragile and ineffective health data protection regime. The future of health data is EHR, and therefore it's imperative that we have a sound and robust framework that facilitates and at the same time regulates its implementation.

Additionally, frequent talks, deliberations, conferences, and roundtables involving numerous stakeholders from the healthcare industry, insurance companies, patient advocacy groups, and the government at the international level are necessary. This would assist in the development of a comprehensive strategy that would aid in the efficient and collusive protection of privacy in the healthcare sector.

6.3 SUGGESTIONS

In the light of the research undertaken and conclusion drawn, the researcher put forth the following suggestions for the adoption and regulation of EHR-

Blockchain in EHR-Security concerns for electronic health data is becoming more severe as malware and ransomware spread. The alarming fact is that the genuine level of cybersecurity risk in electronic health systems is significantly underreported.[215]Incorporating blockchain technology into healthcare can solve some of the existing problems in Electronic Health Records. Blockchain technology is intended to facilitate connection by distributing data across an open network. By distributing patient data throughout a peer-to-peer network, blockchain eliminates the dangers associated with centralized storage of health records. With a distributed ledger, transaction issues are avoided because when one data block is altered or modified, it becomes invalid, invalidating the subsequent set of chained data blocks. The advantage of blockchain technology is its security. The data included in a partnership, or the electronic health record, can be encrypted using public-key cryptography and decrypted using the private key (password) held by the transaction's owners, the patients. The advantage of blockchain technology is its security. The data included in a block, or the electronic health record, can be encrypted using public-key cryptography and decrypted using the private key (password) held by the transaction's owners.[216]Blockchain technology enables the validation of clinical trial and claim outcomes, the tracking of medication, the authentication of prescriptions, and the prevention of insurance fraud. Additionally, smart contracts may leverage blockchain to take action based on preset outcomes, minimizing the need for human

[215]Leo Scanlon, Deputy Chief Information Security Officer For The U.S. Department Of Health And Human Services. (2017, June 8). Comments before the U.S. Congress, House Energy and Commerce Committee. Washington, DC.
[216]Sarah J. Tomlinson Donna K. Hammakernna Yilmaz C. Kaymak,5th Eds, HEALTH RECORDS AND THE LAW, (Jones & Bartlett Learning LLC, 2019)

intervention. Although the usage of blockchain technology is still in its infancy, some EHRs have already integrated it to assure security, scalability, and confidentiality.[217]

Adoption of EHR should be incentivized-Whenever a significant change is to be brought into the system, it is seen that incentive programs are implemented internationally to encourage private players to embrace it in accordance with government requirements. No such incentives are included in any of India's planned EHR initiatives. One of the reasons for this could be reliance on Public-Private-Partnerships or Government Funded Health Insurance Schemes to drive such adoption. India's healthcare system is fragmented, posing measurement and economic problems. To encourage adoption, the government must offer funding and an enabling environment for stakeholders. Given the current low level of government expenditure on health, it is prudent to prioritize investment in the fundamental building blocks of data creation, both through legislation and finance. The government must provide some kind of incentive to initiate EHR adoption by private players.

Phase-by-phase implementation-The adoption and meaningful use of technology should be introduced in a phase-by-phase manner through the use of the law. Rather than concentrating on a comprehensive law to be formulated at the first instance, the law should comprehend the changing need. When a drastic change is brought to the existing system, there should be a strong support mechanism that regulates and promotes the change simultaneously.

Need for an international framework- Just like we have Trade-related aspects of Intellectual property rights (TRIPS) to finetune the IP regime across the globe, it would be great to formulate an international standard common to all nations when it comes to collecting and maintaining EHR. Currently, we have an Electronic Health record manual for developing countries which was brought out by World Health Organization (WHO).[218] Though it prescribes some measures to be adopted while implementing the EHR system, it doesn't enforce. Therefore, most countries have not given due consideration to this manual.

---

[217]DivyaDugar , *Future of Electronic Medical Records: Experts Predict EMR Trends in 2021*, SELECTHUB, https://www.selecthub.com/medical-software/emr/electronic-medical-records-future-emr-trends/ , accessed on August 10.

[218]Electronic Health Records: Manual for Developing Countries , 2006, ISBN 92 9061 2177 (NLM Classification: WX 173) ,World Health Organization 2006

Progressive legal framework- There is a need for standardized legal framework for the collection, usage, and storage of electronic health data, which could be used across all kind of healthcare institution, thereby allowing healthy and safe exchange of standardized data, without compromising on patient privacy. Privacy Impact Assessments are also required for clinical trials, research projects, and biological data collection. Patients should be given the privilege and authority to delete their health information. There should be proper guidelines on how long and in what format health data should be stored and maintained. Healthcare institutions should not be allowed to maintain records for lengthy periods, as this frequently results in illegal access to and subsequent abuse of such data. Provisions for notifying data breaches should be introduced just like that of United states, so that the patients can take informed decisions. There is an inevitable need to include safeguards that regulate the security of patient data once it is accessible by other parties like as insurance companies. While physicians in the Indian context and insurance companies frequently have unrestricted access to a patient's medical records, there is a glaring lack of safeguards to ensure that this information is not released to or accessed by unauthorised individuals within these insurance companies or outsourced consultants. Individuals should be given to retain their anonymity while transacting with specialized healthcare organizations. A critical way to address public concerns about the potential for unauthorized use of personal information gathered for research is by issuing confidentiality certificates similar to those issued in the United States to safeguard sensitive information on research participants from forced disclosure.[219]

Therefore, the researcher considers that it's high time that we should have a progressive legislation that could regulate and incentivize EHR adoption in India.

[219]GUIDANCE ON CERTIFICATES OF CONFIDENTIALITY, OFFICE OF HUMAN RESEARCH PROTECTIONS, U.S DEPARTMENT OF HEALTH AND HUMAN SERVICES available at http://www.hhs.gov/ohrp/policy/certconf.pdf [last visited on 21st July, 2021].

7. BIBLIOGRAPHY

GOVERNMENT NOTIFICATIONS

1. Press Information Bureau, https://pib.gov.in/PressReleasePage.aspx?PRID=1693225
2. Notification of Electronic Health Records (EHR) Standards 2016 for India, MoHFW Circular No. Q11011/3/2015eGov(30/12/2016)

ARTICLES

1. Abha Agrawal, *Medication Errors: Prevention Using Information Technology System*, British Journal of Clinical Pharmacology
2. Barnett GO. *The application of computer-based medical-record systems in ambulatory practice*. 310 N Engl J Med.
3. Edward Shils, *Privacy: Its Constitution and Vicissitudes*, Law & Contemporary Problems
4. FaraAninha Fernandes, Georgi V Chaltikyan, *Analysis of Legal and Regulatory Frameworks in Digital Health: A Comparison of Guidelines and Approaches in the European Union and United States,* Journal of the International Society for Telemedicine and E health
5. Fouzia F. Ozair and others, *Ethical Issues in Electronic Health Records: A General Overview*, PICR
6. GeylaniKardas, E. TurhanTunali, *Design and implementation of a smart card based healthcare information system*, Journal of Elsevier, Computer Methods and Programs in Biomedicine
7. Harleen Kaur, *Electronic Health Records in India: Legal Framework and Regulatory Issues*, RGNUL Student Research Review
8. Harleen Kaur, *Electronic Health Records in India: Legal Framework and Regulatory Issues,* RGNUL Student Research Review
9. Ismail Keshta, Ammar Odeh, *Security and Privacy of Electronic Health Records: Concerns and Challenges*
10. J. Frazee, M. Finley, JJ Rohack, *mHealth and Unregulated Data: Is this Farewell to Patient Privacy*, Indiana Health Law Review
11. Jyotiranjan Mallick, *Digital information security in Healthcare Act: Its impact on m-health vis-à-vis Personal Data Protection Bill, 2019*, NLUJ LAW REVIEW

12. Kumar, A., Jeyalakshmi, S., Mukhopadhyay, K.P. & Gupta, P., *Improving and strengthening the use of ICD 10 and medical record system in India.* Central Bureau of Health Intellegence, New Delhi.
13. Lauren Jacques, *Electronic Health Records and Respect for Patient Privacy: A Prescription for Compatibility,* Vanderbilt Journal of Entertainment and Technology Law
14. Lowell Vizenor, Barry Smith, Werner Ceusters, *Foundation for the Electronic Health Record: An Ontological Analysis of the HL7's Reference Information Model*
15. Manisha Mantri, R. Rajamenakshi, Gaur Sunder, *Addressing Data Privacy in Digital Health: Discussion on Policies, Regulations and Technical Standards in India*
16. Milind Antani, Darren Punnen, Shreya Shenolikar, *Digital Health in India- Legal, Regulatory and Tax Overview*
17. N. Anju Latha, B. Rama Murthy, U. Sunitha, *Electronic Health Record, International Journal of Engineering Research & Technology*
18. N. P. Terry, *Symposium: The Politics of Health Law: Under-regulated Health Care Phenomena in a Flat World: Medical Tourism and Outsourcing,* Western New England Law Review
19. Panagariya, Ashok, *The Challenges and innovative solutions to rural health dilemma,* Annals of Neurosciences
20. Patel VL, Arocha JF, Kushniruk AW. *'Patients and physicians' understanding of health and biomedical concepts: relationship to the design of EMR systems*, Journal of Biomedical Information
21. Patrick Kierkegaard, *Electronic Health Record: Wiring Europe's Healthcare*, Computer Law & Security Review
22. Paul C. Tang, Joan S. Ash, David W. Bates, J. Marc Overhage, Daniel Z. Sands, *Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption*, Journal of American Medical Informatics Association
23. R.Venkata Rao, Subha Rao (eds), *A Public Disclosure on Privacy – An Analysis of Justice K.S. Puttaswamy v. UOI*, NLSIU, Bangalore
24. Rahimi, B., Vimarlund, V., and Timpka, T., *Health information system implementation: A qualitative meta-analysis,* Journal of Medical Systems
25. Ryan M. Krisby, *Health Care Held Ransom: Modifications to Data Breach Security & The Future of Heath Care Privacy Protection*, Health Matrix: Journal of Law-Medicine

26. Sarbandhikari Suptendra Nath, *Digital Health in India – As envisaged by the National Health Policy*, BLDE University Journal of Health Sciences
27. Shahidul Islam Khan, Abu Sayed & Latiful Hoque, *Digital Health Data: A Comprehensive Review of Privacy and Security Risks and Some Recommendations*, Computer Science Journal Of Maldova
28. SharonaHoffman&AndyPodgurski, *In Sickness,Health,andCyberspace:Protecting the Security of Electronic Private Health Information*, B.C. L. REV
29. Terry NP, *Privacy and the Health Information Domain: Properties, Models and Unintended Results*, European Journal of Health Law
30. Tracy D Gunter, Nicolas P Terry, *The Emergence of National Electronic Health Record Architecture in the United States and Australia: Models, Costs and Questions*, Journal of Medical Internet Research
31. Wendy K. Mariner, *Reconsidering Constitutional Protection for Health Information Privacy*, University of Pennsylvania Journal of Constitutional Law

BOOKS

1. E. MOSSIALOS, G. PERMANAND, R. BAETEN & T. K. HERVEY, HEALTH SYSTEMS GOVERNANCE IN EUROPE: THE ROLE OF EUROPEAN UNION LAW AND POLICY (Cambridge University Press, 2010)
2. Electronic Health Records: Manual for Developing Countries , 2006, ISBN 92 9061 2177 (NLM Classification: WX 173) ,World Health Organization 2006
3. INSTITUTE OF MEDICINE, BEYOND THE HIPAA PRIVACY RULE : ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH (National Academies Press 2009)
4. MARGARET AMATAYAKUL, HANDBOOK FOR HIPAA-HITECH SECURITY 84 (American Medical Association 2013)
5. P. ROOM & F. F. WATERHOUSE, BUTTERWORTHS DATA SECURITY LAW AND PRACTICE 68 (Butterworths Law, 2009)
6. Sarah J. Tomlinson Donna K. Hammakernna Yilmaz C. Kaymak,5th Eds, HEALTH RECORDS AND THE LAW, (Jones & Bartlett Learning LLC, 2019)
7. V.N. SHUKLA, CONSTITUTION OF INDIA 754 (11th edn, Eastern Book Company 2008).

8. WHO 2006, ELECTRONIC HEALTH RECORDS: MANUAL FOR DEVELOPING COUNTRIES**,** ISBN 92 9061 2177

STATUTORY PROVISIONS

1. Constitution of India, Part XVIII, Emergency Provisions
2. Data Protection Act, 1998, §1(1), c. 29 of 1998, Acts of Parliament, 1998 (UK)
3. Data Protection Directives
4. Digital Information Security in Healthcare Act (DISHA), 2018
5. Epidemic Diseases Act 1897, No.3, Acts of Parliament, India (1897)
6. Health Data Management Policy, 2020
7. Health Insurance Portability and Accountability Act, Pub. L. 104-191
8. HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414
9. Indian Penal Code 1860, §269, No. 45, Acts of Parliament, India (1860)
10. Medical Termination of Pregnancy Act, 1971, No. 34, Acts of Parliament, India (1971)
11. Right to Information Act, 2005, No.22, §8(1), Acts of Parliament, India, (2005)
12. Privacy and Confidentiality, National Ethical Guidelines for Biomedical and Health Research involving Human Participants Rule, 2017
13. Mental Healthcare Act, 2017
14. The Pre-Natal Diagnostic Techniques (Regulation And Prevention Of Misuse) Amendment Act, 2002
15. General Administration Requirements, 45 C.F.R. §160 (2016) and Security and Privacy, 45 C.F.R. § 164 (2016).
16. Telemedicine Guidelines, 2020
17. The HIPAA Privacy Rule
18. The Indian Medical Council (Professional Conduct, Etiquette and Ethic) Regulations, 2002
19. The Personal Data Protection Bill, 2019
20. The Privacy Act, 1988, No. 119, Acts of Parliament, 1988 (Australia)
21. UK Data Protection Act, 1998, c. 29 of 1998, Acts of Parliament, 1998 (UK)
22. Clinical Establishment (Registration and Regulation) Act, 2010

REGULATIONS

1. HIPAA Security and Privacy Regulations, 2018, §§160.101 and 164.104

2. Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulations, 2002

OTHERS

1. Agency for Healthcare Research and Quality, 2009, *Report on State Medical Record Access Law*
2. Annual report 2020-21, Department of Health & Family Welfare Ministry of Health & Family Welfare
3. Kathryn C. Montgomery and others, *Health Wearable Devices in the Big Data Era : Ensuring Privacy, Security, And Consumer Protection*, CDD Report, 2017, DEMOCRATIC MEDIA
4. Leo Scanlon, Deputy Chief Information Security Officer For The U.S. Department Of Health And Human Services. (2017). Comments before the U.S. Congress, House Energy and Commerce Committee. Washington, DC
5. MARGARET AMATAYAKUL, HANDBOOK FOR HIPAA-HITECH SECURITY (American Medical Association 2013)
6. National Ethical Guidelines for Biomedical and Health Research involving Human Participants, 2017

WEBSITE

1. *A Survey of Primary Care Doctors in Ten Countries Shows Progress in Use of Health Information Technology, Less in Other Areas,* (2017), HEALTH AFFAIRS, https://www.healthaffairs.org/doi/abs/10.1377/hlthaff.2012.0884
2. Administrative Security Rule, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/
3. Australian Government, *Office of the Australian Information Commissioner*<https : //www.oaic.gov.au/privacy/the-privacy-act/health-and-medical-research/
4. Chennupati K. Ramaiah, Surya Prakash Gulla, *Electronic Medical Records Management Systems: An Overview*, https://www.researchgate.net/publication/228740128_Electronic_Medical_Records_Management_Systems_An_Overview/link/54ae492f0cf2828b29fccccc/download
5. *Comparing Usability Testing Outcomes and Functions of Six Electronic Nursing Record Systems*, NATIONAL CENTER FOR BIOTECHNOLOGY INFORMATION, https://pubmed.ncbi.nlm.nih.gov/26878766/

6. Covered Entities and Business Associates, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html
7. COVERED ENTITIES AND BUSINESS ASSOCIATES, US DEPARTMENT OF HEALTH AND HUMANS SERVICES, https : //perma.cc/4SWX-KLBH
8. Digbijay Mishra & Madhav Chanchani, *For the first time, India has more rural net users than urban*, TIMES OF INDIA, https://timesofindia.indiatimes.com/business/india-business/for-the-first-time-india-has-more-rural-net-users-than-urban/articleshow/75566025.cms
9. DivyaDugar , *Future of Electronic Medical Records: Experts Predict EMR Trends in 2021*, SELECTHUB, https://www.selecthub.com/medical-software/emr/electronic-medical-records-future-emr-trends/
10. Electronic Health Record Error Prevention Approach Using Ontology in Big Data', (2015), http://webpage.pace.edu/kg71231w/docs/HPCC2015-1.pdf
11. Electronic Health Record Standards, https://www.nhp.gov.in/NHPfiles/EHR-Standards-2016-MoHFW.pdf
12. Electronic Medical Record Systems', https://digital.ahrq.gov/key-topics/electronic-medical-record-systems#one
13. GUIDANCE ON CERTIFICATES OF CONFIDENTIALITY, OFFICE OF HUMAN RESEARCH PROTECTIONS, U.S DEPARTMENT OF HEALTH AND HUMAN SERVICES available at http://www.hhs.gov/ohrp/policy/certconf.pdf
14. HIPAA Security Series: Part2, U.S. DEP'T OF HEALTH & HUM. SERV., 9 (March 2007), https://www.hhs.gov/sites/default/files/ocr/ privacy/hipaa/administrative/securityrule/adminsafeguards.pdf
15. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf.
16. KashishAneja and Nikhil Pratap, *Implement Arogya Setu but Only through Law*, THE HINDU, https : //www.thehindu.com/opinion/op-ed/implement-aarogya-setu-but-only-through-law/article31391708.ece
17. Kim Zetter, *Why Hospitals are the Perfect Targets for Ransomware*, WIRED https://www.wired.com/2016/03/ ransomware-why-hospitals-are-the-perfect-targets/.
18. ManaviKapur, *The Corona Virus App Narendra Modi Endorsed is a Privacy Disaster*, QUARTZ INDIA, , https : //qz.com/india/1838063/modis-aarogya-setu-coronavirus-app-for-india-a-privacy-disaster/

19. Markle Foundation, *The Personal Health Working Group*, https://web.archive.org/web/20070104212409/http://www.connectingforhealth.org/resources/final_phwg_report1.pdf
20. National Digital Health Mission, https://ndhm.gov.in/, accessed on 18th May, 2021
21. National Health Portal India, https://www.nhp.gov.in/nhpfiles/national_health_policy_2017.pdf
22. National Health Profile, 25th June, 2019, http://www.cbhidghs.nic.in/showfile.php
23. Peter Garratt, Joshua Seidman, *EMR vs. HER- What is Difference*, https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference
24. Ruby Sahney, *Mukesh Sharma, Electronic Health Records: A General Overview, (*2018), https://www.academia.edu/37262485/Electronic_health_records_A_general_overview
25. Sandhya Keereli, *Internet penetration rate in India from 2007 to 2021,* STATISTA, https://www.statista.com/statistics/79074/india-internet-penetration-rate/
26. Integrating Privacy & Security into Your Practice, HEALTH IT, https://www.healthit.gov/providersprofessionals/ehr-privacysecurity/practice-integration.
27. National Health Stack: Strategy and Approach, NITI Aayog, Government of India, available at https://niti.gov.in/writereaddata/files/document_publication/NHS-Strategy-and-Approach-Document-for-consultation.pdf
28. Shanthi S, India *Ranked Third Worst For Data Privacy In Global Surveillance Index*
29. Soutik Banerjee and others, *Privacy in Times of Corona : Problems with Publication of Personal Data of COVID-19 Victims,* LIVE LAW, https : //www.livelaw.in/columns/privacy-in-times-of-corona-154360?infinitescroll=1
30. Statista.com, Internet usage in India - statistics & facts, Published by Sandhya Keelery
31. Tanvi Mani, *Privacy in Healthcare: Policy Guide,* The Centre for Internet & Society, https : //cis-india.org/internet-governance/blog/privacy-in-healthcare-policy-guide
32. ThePhysicalSafeguards,http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf

33. Vikram Koppikar, *Covid-19 : Data Privacy in these Testing Times*, MONEY CONTROL: INDIA , https : //www.moneycontrol.com/news/economy/policy/covid-19-data-privacy-in-these-testing-times-5120201.html
34. *What are the differences between Electronic Medical Record, Electronic Health Record and Personal Health Records*,https://www.healthit.gov/faq/what-are-differences-between-electronic-medical-records-electronic-health-records-and-personal
35. World Health Organisation. Sustainable *Development Goals, World Health Organisation (WHO),* https://www.who.int/sdg/targets/en/

APPENDIX

CERTIFICATE ON PLAGIARISM CHECK

1. Name of the Candidate	ASLAM AHAMMED S R
2. Title of thesis/dissertation	LEGAL REGULATIONS OF ELECTRONIC HEALTH RECORDS: A COMPARATIVE PERSPECTIVE
3. Name of the supervisor	DR. LIJI SAMUEL
4. Similar content (%) identified	9%
5. Acceptable maximum limit (%)	20%
6. Software used	GRAMMARLY
7. Date of verification	OCTOBER 9, 2021

Checked By (with name, designation & signature) :

Name and Signature of the Candidate :ASLAM AHAMMED S R 

Name & Signature of the Supervisor :DR.LIJI SAMUEL