

# Infringement of Medical Data Privacy – A Threat to Human Rights

R.B.Rishabh, H. Rajaram<sup>1</sup>& B. YamunaSaraswathy<sup>2</sup>

## Abstract

Human Rights are the pre-requisites for the existence of man in a society. It has a wide scope and it also includes the basic fundamental rights. It is not possible for all the governments to grant every right as fundamental right in lieu place them under the context of human rights and provide provisions to protect them. In today's society data being easily accessible portrays to be an outright threat. Here the question of privacy creeps into the life of the people and could make their lives disastrous. The most intricate type of privacy infringement would be that of the medical records.

Though we talk about medical privacy it still remains to be a mere theoretical subject rather than being a right which ought to be protected. The technological advancements pave way for safeguarding e-medical records. In today's world, law on medical data privacy is an evolving concept. Developed countries like U.S. and U.K. have enacted laws such as Health Insurance Portability and Accountability Act, 1996 (HIPAA) and Data Protection Act, 2018 (DPA) respectively for protection of personal health information (PHI). In India, medical privacy law is still under the scanner under the proposed name Digital Information Security on Healthcare Act, 2018 (DISHA).

This article aims to cast light upon the concept of medical data privacy as a human right. This article also aims at studying the medical data protection laws in other countries. It aims at analyzing the highlights of the proposed Digital Information Security on Healthcare Act, 2018 (DISHA) in India. Further, it statistically analyzes the medical data breaches. The authors give an insight about the effects of medical data protection laws with regard to human rights and provide suggestions for betterment of such laws.

---

<sup>1</sup>IVth year B.Com.LL.B(Hons.), School Of Excellence in Law, TNDALU, Chennai.

<sup>2</sup>IVth year B.Com.LL.B(Hons.), School Of Excellence in Law, TNDALU, Chennai.

## **Introduction**

Human rights are the cardinal rights of the people underlying minimum standard to live with equality and dignity. Human rights are of wider scope and subsume all kinds of rights necessary for a person to lead his life peacefully. Privacy is one of the integral aspects of human rights. Article 12 of the Universal Declaration of Human Rights and Article 17 of International Covenant on Civil and Political Rights states that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks”. In an ever upgrading society, the privacy of people has become a prey to the technological developments and advancements. Like a human attitude has two extremes, these developments can be a boom or bane to the society. When a person’s information becomes available to anyone around the world, it can lead to piercing his privacy. In this way, his basic human right of leading his life with dignity can be infringed. In the current scenario, privacy invasion trend has turned its head at medical data. Nowadays, the medical information of patients is stored by the hospitals digitally for betterment of its services. But such information is not impregnable at all times. Furthermore, in some countries, this information is accessible by the employers of such patients and their medical insurance companies as well. This makes their Personal Health Information (PHI) available to umpteen numbers of people. Any unscrupulous use of such PHI for other purposes outside this sector can be detrimental and scandalous to an individual. Hence, there is an exigency for reinvigorating the existing laws for protection of medical data privacy.

## **Research Questions**

1. What is the nexus between right to privacy and human rights?
2. What is the current scenario of medical data protection around the world and how it infringes human rights?
3. What are the important provisions proposed by the recent Digital Information and Security in Healthcare Act, 2018 (DISHA)?
4. Whether the proposed DISHA will have effective changes in Indian healthcare sector?
5. What are the reasons for medical data breaches despite of stringent laws?

## **Objectives of the Study**

1. To interpret the right to privacy with regard to human rights.

## **Human Rights vis-a-vis Justice System in Present Era : A Publication of Jus Dicere**

2. To know about the current scenario of medical data protection including its legislations and how its breach infringes human rights.
3. To study the recently proposed medical data privacy legislation (DISHA) in India.
4. To find out whether the proposed law (DISHA) can be implemented effectively.
5. To analyze the reason for medical data breaches despite of stringent laws and to suggest some modifications that can be made in the medical data protection legislations.

### **Research Methodology**

The method of research which the authors have used is a doctrinal research, it includes an analytical study of the provisions of The Health Insurance Portability and Accountability Act, 1996 (HIPAA), Data Protection Act, 2018 (DPA) and Digital Information and Security in Healthcare Act, 2018 (DISHA – Proposed), a comparative study which includes the comparison of right to privacy in healthcare sector by referring to the international conventions on human rights, an exploratory study which includes the analysis of healthcare data breaches, and a formulative study which includes our own findings in this area.

### **Laws in Developed Nations**

#### **United States of America**

In the last four decades there has been a dynamic shift in the US healthcare industry, which was driven by the changes in the information technology and also by the enactment of new laws pertaining to this subject matter. The Health Insurance Portability and Accountability Act (HIPAA), 1996 was passed to standardize the medical records and the health insurance sector in national level. The privacy rules of HIPAA focus on the use and disclosure of patients records by the “covered entities”. These entities must ensure implementation of check measures to safeguard and control the intra and inter organizational information access. The features of HIPAA to be highlighted include complete power of an individual over his information, to restrict the use and release of Personal Health Information (PHI). People have absolute right over their information and can decide on matters relating to sharing of details. It also presses upon the factor that the consent given by an individual shall be out of his free will and there shall be no signs of undue influence. A person’s personal information can be used for health purposes only but there are certain exceptions to the general rule. The act also

mandates proper procedures to protect privacy and provides to appoint a privacy official for the grievances to be addressed.

Despite having a federal act, the state of California has enacted a separate law for medical data protection having stringent provisions. The act passed by the state California is called as Confidentiality of Medical Information Act (CMIA). This act imposes huge fines on individuals for breach of medical record's confidentiality or otherwise using of data for purposes other than for which the consent is acquired.

### **United Kingdom**

Though there is no special act for Medical Data Protection in UK still they have a pivotal and a wider act dealing with data protection known as the Data Protection Act (DPA) of 2018 which incorporated EU General Data Protection Regulation (GDPR), 2018 into law in the UK. The UK act focuses on the confidentiality and management of personal data of consumers. The act also concentrates on special category of privacy rights like purpose of research, public health and journalism are protected as per the GDPR provisions. The consent of the consumer is required to transfer the data, as per this act children above the age of 13 can give consent, for sharing of his data with others.

### **Comparison of HIPAA and GDPR**

The HIPAA of US and the GDPR of EU has many similarities in governing of the medical data. Both the laws mandate stringent protection of medical data ensuring proper maintenance of records and to adhere with the protocols established while disposing data. The difference between the two can be studied on the topic of consent. Under HIPAA there is no requirement to get consent of the individuals to store and process the data, if it is done securely. Under GDPR it is mandatory to get consent to store medical data of individuals. Both HIPAA and GDPR impose stringent penalties for violation of its regulations. HIPAA guidelines may be waived in case of natural calamities but there are no such provisions in GDPR. Although GDPR is not restricted to healthcare it is more stringent as it brings in better protection to the resorted than HIPAA.

### **Emerging Medical Records Privacy Law in India**

At prima facie records or data were held in physical form and now they are being held in an electronic format, the manner or form in which the data being held have come a long way all credits to the technology advancements. Presently there has emerged the need to secure the data in order to save the privacy of patients. The term data protection was evolved by the efforts of the European Union in the mid-1950s. Thereafter, there has been umpteen numbers

## Human Rights vis-a-vis Justice System in Present Era : A Publication of Jus Dicere

of legislations passed by various developing nations. India only recently has felt the need of digital data protection act especially in healthcare sector. In spite of having general laws like Information Technology Act, 2000 for data protection, a sudden urge to draft a special legislation was felt because right to privacy was made a fundamental right in India. The proposal for this legislation was made by the Ministry of Health and Family Welfare (MoHFW). Not only does the MoHFW stops with drafting the legislation (DISHA) but also proposes to constitute a nodal body called “National Electronic Health Authority” (NEHA) which would take up and provide e-health standards. It also deals with matters pertaining to privacy, safeguards of e-health and take up the responsibility of safe keeping and exchange of e-health records. The recommendations for DISHA were made by a committee of experts headed by former Supreme Court Justice B.N.Srikrishna (White Paper).<sup>3</sup> The committee recommended that a data protection law must be flexible and indifferently applied to both private and public sector. One of the most important provisions of DISHA is that the healthcare organization must get a genuine consent from its patients by making them aware of digitalized medical data before use or transfer of such data. Such consent given by the individuals can be withdrawn at any time. This provision is really a new one in the healthcare data protection concept compared to the laws in other countries. And it is hoped that such strong provision will help in effective application of the law. This act also gives the patients the right of refusal of consent and no undue influence must be casted on such a right so as to be eligible for basic medical needs. DISHA also provides for imprisonment if the concerned organization does not notify its patients about the data breach within 3 days. Furthermore, the scope of the term ‘commercial purpose’ in the proposed act is wider so as to provide prodigious control to the people over their data. Despite the fact that the act needs to be re-explored at many parts, it will be extremely effective and helpful once it is enforced after making some modifications. And in a developing and well-populated country like India, it is important to encrypt all medical data files and to have a complex cyber security system as a simple breach can lead to privacy intrusion and identity theft of millions of people. Thus, the proposed DISHA has given high expectations to the individuals for screening the virtual medical data and is hoped to improve the panorama of privacy as human rights in India.

---

<sup>3</sup>SupratimChakraborty, *DISHA to give direction to digital information security in healthcare*, THE ECONOMIC TIMES (May. 02, 2018), <https://health.economictimes.indiatimes.com/news/industry/disha-to-give-direction-to-digital-information-security-in-healthcare-supratim-chakraborty/63993563>.

## **Medical Data Breaches**

With the escalating growth of health sector, the threat of data breach is also increasing. The health sector has become a lucrative prey for the hackers as they can get a huge amount of vulnerable data. The stolen information includes a person's name, social security number, bank account number, credit card details and even physical addresses which can be easily used for identity thefts. This leads to infiltration in a person's privacy and infringes his human rights to a greater extent. And the most lucrative menace here is that the hackers also steal information such as pharmaceutical processes and drug formulas which can be sold for billions of dollars. This not only affects the concerned organizations but also people at large if it's in the hands of nefarious people. So it is important for the government to enact stringent laws in respect of healthcare data breaches inculcating provisions regarding human rights as there is a great threat to a person's privacy. And the healthcare organizations should also make strong precautions and have recurring inspection policies so as to avoid breach of such data.

Irrespective of such stringent precautions, the hackers always have found their way to loot the information as there is some kind of flaw in the safeguard mechanism. Such breaches have led to the release of millions of data records in the last five years. And the largest breach ever made in healthcare sector is the breach of Anthem Health in the year 2015. This incident shook the entire healthcare sector as nearly 78.8 million patient records had been stolen.<sup>4</sup> Besides, it has been said that those stolen records were mostly used for the purposes of identity theft. This mainly happened because of the laxity on part of Anthem Inc., to encrypt its files.

In India, according to global digital security firm Gemalto's "Breach Level Index", the healthcare industry accounted for 28 percent of data breaches in 2016 raising 11 percent compared to 2015. It is said that the healthcare data breaches often happen as a consequence of insider's actions rather than by an external hackers, as these insiders know how to manipulate the flaws in the cyber security made by the organizations. On this wise, it can be clearly seen that the healthcare sector is like meat and potatoes to the hackers for intrusion. Mostly in healthcare organizations, multiple layers of data security are not built as it complicates the work of employees and leads to chaos. Hence, this stance must be changed by the healthcare organizations as the data breach in this sector is increasing at a rapid pace.

---

<sup>4</sup>Nate Lord, *Top 10 Biggest Healthcare Breaches of all Time*, DIGITAL GUARDIAN (June 25, 2018), <https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time>.

### **Suggestion**

1. The healthcare organizations must have an effective check over their employees so as to avoid insider data breach.
2. Such organizations must have multiple layers of cyber security to protect its information thereby making it impenetrable.
3. There must be a strong encryption of data files and recurring check of such data by the organizations.
4. The laws enacted in this regard must not only apply for covered entities but for all the areas under healthcare sector.
5. Such laws must provide for a higher penalty or imprisonment provisions to those who breach the medical data so as to reduce such threat.
6. The quantum of data acquired by insurance companies must be just and reasonable.
7. Medical data protection laws must pave way for the protection of human rights.

### **Conclusion**

From Hippocratic Oath to Right to be forgotten, the importance of right to privacy and confidentiality in medicine has been mentioned theoretically by various authors and in many medical laws. Right to privacy in recent days is an evolving concept which is trying to catch up with the technological advancements, in order to make the term 'Privacy' exist in this technologically infringing society. Though we enjoy the fruits of the available technological advancements we also end up getting infringed by the abuse of such technology. Furthermore, the transformation of medical data from papers to digitalization has spurred the need for special laws focusing on not only data protection but also on the privacy of individuals. Nowadays, people are made aware of threats and invasion of their privacy by way of data breaches but such awareness still has a long way to go and should touch roots (lower-class) of the society. This has compelled the governments around the world to enact new laws in this aspect and it is important to enact special laws for healthcare data as it has the most sensitive personal data starting from birth date of a person to his genetic diseases. Nonetheless, right to privacy is one of the core aspects of human rights. So the breach of a medical data not only results in invasion of his privacy but also violation of his basic human rights. Hence, it is important for the governments to endorse the importance of human rights while drafting legislation in this regard.