HEALTHCARE DATA PROTECTION LAWS IN INDIA: AN OVERVIEW

Shuvangi Gupta*

ABSTRACT

This paper aims at discussing legislation pertaining to the healthcare system of India and other countries along with the importance of privacy for ethical reasons. It is important to protect a person's right to privacy as it is a Fundamental Right under Article 21 of the Indian Constitution, established by the Supreme Court in Justice K.S.Puttaswamy (Retd) vs Union Of India, 2018. In this paper, I have delved into the intricacies of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, outlining its provisions, regulations, and enforcement mechanisms. The three components of HIPAA are security rule compliance to keep the data of patients safe and require healthcare organisations to exercise: administrative, physical, and technical security. In September 2016, the Ministry of Health and Family Welfare (MoHFW) announced electronic health record (EHR) standards for India. Clinical establishments are increasingly using electronic medical records (EMR) and electronic health records (EHR) as the preferred method of storing patient information. For example, the disclosure that an individual is infected with HIV or another type of sexually transmitted infection can cause social isolation and/or other psychologically harmful results. Finally, security breaches could put individuals in danger of identity theft.

INTRODUCTION

With the advent of digitisation in our country and increasing usage of mobiles, laptops and artificial intelligence, it is the need of the hour to bring in stringent legislations to protect the sensitive personal data of participants in any research and patients going in for treatment at hospitals. This paper aims at discussing legislation pertaining to the healthcare system of India and other countries along with the importance of privacy for ethical reasons.

Why Data Protection laws are needed in healthcare?

Governments all over the world have acted to create a digital identity ecosystem, as the need of the present times is to go beyond paper and store data electronically and more efficiently for storing biometric data documents that may help in distinguishing one patient from the

*BA LLB, FOURTH YEAR, ST. XAVIER'S UNIVERSITY, KOLKATA.

other and not to confuse one's health care records with another. According to the rules of the Clinical Establishments (Registration and Regulation) Act, 2010 all the clinical establishments which are registered need to maintain the records of all the patients electronically.1 In healthcare settings around the globe, patients are required to give their biometrics either through fingerprints, palm prints or retina identification to unlock their digital medical records. For example, you take your father for a checkup at a multi-specialty hospital that requires your biometrics to access their website which will upload the test results. As advanced as this may sound, it is equally dangerous for a person's privacy and security and needs to be preserved and protected from any kind of data manipulation. It is important to protect a person's right to privacy as it is a Fundamental Right under Article 21 of the Indian Constitution, established by the Supreme Court in Justice K.S.Puttaswamy (Retd) vs Union Of India, 2018. Clinical establishments are increasingly using electronic medical records (EMR) and electronic health records (EHR) as the preferred method of storing patient information. According to Section 43A of the Information Technology Act (ITA), any body-corporate that possesses, deals or handles any "sensitive personal data" or information

India's Initiative: DISHA

Disha means a direction in the Hindi language, with the goal of providing a direction to e-healthcare data storage Indian government has taken several steps for digital health data privacy, security, standardisation, and confidentiality. In 2016, the Ministry of Health and Family Welfare (MoHFW) announced electronic health record (EHR) standards for India. Academicians, government officials and technologists were on the committee that developed the recommendations and in addition to professional entities, regulators and stakeholders several technology and social commentators submitted the standards for review. In 2016, the EHR Standards were revised in response to input from a variety of stakeholders. According to the MoHFW proposal, the Digital Information Security in Healthcare Act (DISHA) would establish a national digital health authority to promote and implement e-health standards, protect patient privacy and security and regulate the storage and sharing of electronic medical records. The MoHFW's National Digital Health Authority is a proposed organisation charged with creating an integrated Indian health information system. One of the organisation's primary objectives is to assist India in its digital health journey and subsequent realisation of

[1] i Rule 9 (iv), The Clinical Establishments (Registration and Regulation) Act, 2010.

Indian clinical terminology (ICT) health sector benefits.[2]The Ministry of Health and family welfare had put in place a draft of the Digital Information Security in Healthcare Act (DISHA) which was passed in 2018. The law is meant to protect digital health data.

The key provisions of DISHA, 2018 are ownership of digital health data, rights of the owner of DHD (digital health data), the duty to secure information, purposes for which DHD can be processed, requirements to be satisfied for data transmission, conditions required for accessing data, provisions on breach of data and adjudicating authorities for the redressal of various offences under this act. India is supposed to become the most populous country by 2023. It is extremely difficult to store data of such a large population in a standardised form and hence DISHA will help achieve the same and improve the easy transfer of patient's health data and establish Health Information Exchanges throughout the country from one health establishment to another. India has governments at two levels that is the Centre and the State, it would be appropriate to establish digital health authorities and both these levels; at the centre, National eHealth Authority and at the state level State eHealth Authority.[3] The data will be stored centrally and the ownership of the data will live with the patient itself, the provisions specifically state that the patients should have the sole right to consent to the use of the data and without that explicit consent sensitive personal information cannot be used.[4]The act describes two types of breach: breach and serious breach. A breach is when the collection of data is not done properly or is unsecured or not according to the guidelines and a serious breach is when sensitive personal data is used for activities that are fraudulent in nature. There is serious punishment under the drug for any breach which includes imprisonment for five years and a fine up to 5,00,00 rupees.[5]We may say the penal provision was inspired by section 72A of the Information Technology Act, 2000, which says disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years and fine extending to Rs 5,00,000.

[2] In brief: Digital healthcare in India. < https://www.lexology.com/library/detail.aspx?g=593f053a-33e6-4bac-8187-34f54f518915> accessed 13th April 2023
[3] The Digital Information Security in Healthcare Act, 2018 S (7)
[4] The Digital Information Security in Healthcare Act, 2018, S (28)
[5] The Digital Information Security in Healthcare Act, 2018, Chapter V.

FOREIGN LEGISLATIONS PERTAINING TO HEALTHCARE: HIPAA

Under HIPAA, the US Department of Health and Human Services (HHS) is required to establish regulations for protecting the privacy and security of health information. Prior to this act, healthcare providers had no security standards in place to safeguard sensitive patient data. As healthcare shifted from paper to electronic records, HIPAA aimed to establish rules that would enable entities to adopt new technologies while still ensuring individual privacy.

HIPAA is comprised of several key rules and standards, including privacy rules, security rules, breach notification rules, unique identifiers role, HITECH act, Transactions and Code sets rule, and omnibus final rules. Compliance with these rules requires healthcare organisations to exercise administrative, physical, and technical security protocols to protect patient data.

The HIPAA Privacy Rule addresses five critical areas related to covered entities and business associates. These include the establishment of new privacy requirements, the application of HIPAA security and privacy protocols, mandatory federal reporting requirements for security breaches, and accounting disclosure regulations.

Unfortunately, HIPAA violations have still occurred, with the most common offences stemming from lack of encryption, unauthorised access, data breaches, loss, theft, and improper disposal of sensitive patient information. In 2016, the largest HIPAA settlement resulted from a security breach that affected 4 million people. A healthcare network in Illinois was found to be non-compliant due to the theft of an unencrypted laptop containing sensitive data on patients. In another case, a Tennessee-based medical imaging company was penalised for having servers that were easily accessible to the public, resulting in the exposure of patient information.

In conclusion, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 remains a critical piece of legislation designed to safeguard patient privacy and security in the healthcare industry. While there have been HIPAA violations over the years, the implementation of these rules has enabled entities to improve patient care while still ensuring privacy in the face of emerging technologies.

PRIVACY: CONSTITUTIONAL AND ETHICAL ASPECT in India

The Fundamental right to privacy is recognized by the Indian Constitution under Article 21 and Article 23 which guarantee the right to life, proper working conditions and maternity relief. The Constitution of India promotes the welfare state under Article 38. In the Kharak Singh vs. State of UP (1962) case, the Supreme Court of India interpreted the right to life broadly to include personal freedom and privacy. The court held that Regulation 236 of the UP Police Regulations violated the Constitution as it infringed upon Article 21 of the Constitution. Maneka Gandhi vs. UOI (1978) laid out a three-pronged test for any law or procedure that interferes with personal liberty, which includes the procedure withstanding the test of fundamental rights conferred by Article 19 and Article 14. It is imperative that the law and procedures authorizing interference with personal liberty and the right to privacy are fair, just and not arbitrary or oppressive. Therefore, it is now well-established that the right to privacy is an integral part of the right to life and liberty under Article 21 of the Constitution of India.

In the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002, Chapter I, also known as the Code of Medical Ethics[6], specific duties and responsibilities of physicians are outlined. Among these is the requirement for physicians to maintain medical records for their indoor patients for a period of at least three years from the commencement of treatment. This should be done in a standard proforma laid down by the Medical Council of India and attached as Appendix 3.

In addition, if any request for medical records is made by the patient or their authorized attendant, or legal authorities, the same should be acknowledged and the documents issued within 72 hours. Physicians are also required to maintain a Register of Medical Certificates giving full details of certificates issued. The identification marks of the patient must be entered and at least one identification mark of the patient on the medical certificates or report must not be omitted. Efforts should also be made to computerize medical records for quick retrieval.

It is important to protect the security of data in health research because of the sensitive and potentially embarrassing nature of the information collected, stored and used. If security is breached, individuals whose health information was inappropriately accessed face a number

[6] The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002,

of potential harms. This includes intrinsic harm as their private information is known by others, economic harm as they could lose their job, health insurance, or housing, and social or psychological harm such as social isolation.

Furthermore, security breaches could put individuals in danger of identity theft. Therefore, it is imperative for physicians and health researchers to ensure that security measures are put in place to prevent unauthorized access to health records and data. This can be achieved through the implementation of strict data protection policies, the use of encryption techniques, and continuous monitoring of access to health records. By doing so, physicians can maintain patient confidentiality and uphold the trust that the public places in them.

According to the case of Mr. X v. Hospital Z (1998), when there is a conflict between two fundamental rights, such as the right to privacy, the right that promotes the public interest or morality takes precedence. The Court acknowledged that while every right has a corresponding duty, there are exceptions to this rule. Therefore, certain instances may arise where there is a right without a corresponding duty. The Court examined the relevant provisions of the Code of Medical Ethics in India and the guidelines on HIV infection and AIDS by the General Medical Council of Britain to investigate the exceptions to the confidentiality rule. The Court found that medical information disclosure is allowed in cases where there is an immediate health risk to others, as in the present case. The right to the confidentiality of the Appellant was not enforceable in this instance because the proposed marriage carried a health risk to a specific individual who was spared from contracting a deadly disease.

COMMENTS

During Covid 19 pandemic, we saw how a person's test result positive or negative can impact public health at large. The concept of quarantine was enforced and had to be abided by the patient and if not would be subjected to punishment under the EPIDEMIC DISEASES ACT, 1897, section 3. The Epidemic Diseases Act lacks procedural guarantees against state power abuse regarding privacy infringement. This has led to concerns about the law being misused for profiling, mass quarantine, and targeting of individuals. Public servants who function under the act are given blanket legal protection, which makes it grossly inadequate when weighed against privacy rights. Therefore, the act does not meet the reasonable restrictions on privacy infringement and needs an urgent overhaul.

I feel that protecting the health care data of a patient is of utmost importance to prevent any sort of societal injury or economic harm, but also there is some protection that needs to be given to the health care providers, that is the doctors, nurses and other health experts involved. During the Covid 19 pandemic years, there have been several instances of threat and injury to doctors, them getting beaten up by the patient's family as they were not able to save the patient and creating a ruckus inside the healthcare institutions.

CONCLUSION

The right to privacy is an integral right of the citizen of India granted by the Constitution, hence it is extremely important to protect it in every possible way. The healthcare sector in the country now has proper legislation which can secure the interest of the patients and any person involved in any clinical trial as a part of the research. The digitalisation of data at an alarming rate calls for stringent measures to protect the subjects of the health industry. With the development of legislation and precedents, healthcare data can now be preserved.