FUTURE OF MEDICAL DATA PRIVACY WITH DIGITAL INFORMATION SECURITY IN HEALTHCARE ACT

Written by ***Akshita Modi***

2nd year B.COM LLB (HONS.), Institute Of Law, Nirma University

ABSTRACT

The right to privacy being an important and intrinsic part of the right to life and liberty also applies to the institutions which are not always state governed. For instance, the health sector in the country should preserve the right of the patient's privacy with regard to personal sensitive medical information. Certain laws should govern the data storage, transfer, and usage in the health sector. It is in this regard only that the following article analysis the new draft of The Digital Information Security in Healthcare Act (DISHA) given by the health ministry. It aims to study existing laws and their drawbacks which the new draft tries to overcome. Further, it determines policy gaps in the given draft for any future changes due to advancement in the technology in the health care sector and endeavours to provide effective recommendations for best governance in the future. Also to create legislation which could specifically govern the health care information in the country? It also aims at fulfilling the objective of securing and governing the health care data of the patients in the best possible way.

INTRODUCTION

The health sector is not deprived of technological advancements. Now all the health records electronically stored. This is beneficial as well as there are certain drawbacks one being privacy and security of health care data. The health care data is regarded as sensitive information of an individual and can be misused and manipulated. For securing this data a country should enact certain laws that could govern the storage, transfer, and security of these electronically stored health care records. In India, there are already existing laws that govern and secure health care data but they are not exclusive for the health sector. India is a highly populated country, it is

difficult to maintain health care records of such a huge population. Due to this, the data is vulnerable to threats to the privacy of patients and the right to privacy being an intrinsic part of the right to life and liberty, it is important to maintain it. The already existing laws are related to some specific areas in the health sector. India needs a law that could govern the health sector as a whole. For the same, the government came up with the draft of an Act which could exclusively govern the health care sector and had tried to remove the flaws in the existing provisions. The article aims at analysing the draft for Digital Information Security in Healthcare Act in reference to the existing laws which it will replace if legislated into law. Also, provide drawbacks in the draft which need to be rectified for better governance in the health sector. The article gives a clear view of future governance in the health sector related to the privacy of personal health care information of patients.

WHY THERE IS NEED FOR MEDICAL DATA PRIVACY?

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[i]. Keeping records electronically is beneficial as it helps in reducing cost; it helps in easy access to the stored data etc. It also helps healthcare organisations to easily use the stored data for many productive purposes. As a large quantity of data is stored it helps government and organisations to make health-related policies, predict epidemics and also helps in inventing new drugs. But as this data is easily assessed it can easily be manipulated. Today commercialisation of data is done on a large scale. The health data include personal information of patients which they might not want to disclose. This personal data is sold by many hospitals to the data-mining companies which in turn resell this data to insurance companies or any other organisation which may misuse this for their benefit. As the electronic medical record helps the government in many ways it cannot be stopped. Instead, it is better to provide protection against any privacy breach to the patients, giving control of their personal sensitive medical information in their hands. The data should be used after the consent of the patients. In India, there are many health data breach cases as the data is stored and processed electronically. There is a need for securing health information of patients in India. There are many existing laws that govern health data protection but these suffer many flaws.

EXISTING LAWS RELATED TO MEDICAL DATA PRIVACY

There are certain Acts and laws which govern personal sensitive data of patients. But the data creation and storage have become very complex therefore the existing laws do not fulfil the purpose. The sensitive personal data which is stored, transferred or handled electronically is subjected to the set of rules under the Information Technology Act, 2000. This data is governed under Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (the 'Data Protection Rules'). This Act restricts its application only to body corporates. Section 43A of this Act says that if anybody corporates who are maintaining any personal sensitive data of any person if fails to safeguard that data then it will require compensating the affected person[ii]. But there are many hospitals and clinical establishments that are not body corporates as section 2(c) of the Clinical Establishment (Registration and Regulation Act, 2010) does not require to incorporate clinical establishments.[iii] There are many clinical establishments do not fall under the preview of section 43A of IT Act, 2000. There are also certain provisions under medical laws that govern the privacy of information. The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 governs the confidentiality of personal data between the medical practitioner and patients[iv]. Under these provisions, medical practitioners are required to maintain confidentiality of patient's information provided during the procedure. But under these provisions, such information may be revealed if required by law or there is any serious threat to a particular community or individual. Disciplinary actions have to been taken for any violation under the provisions. There are certain specific laws that govern particular medical information. The Medical Termination of Pregnancy Act, 1971 has provisions for maintaining the confidentiality of information related to the termination of pregnancy between the patient and the doctor. This Act prohibits the doctors to disclose any information under the admission register to any other person[v]. Also, the admission register is stored under the safe custody of the hospital's head. The privacy of patients suffering from HIV is safeguarded by the Human Immunodeficiency Virus and Acquired Immune Deficiency Syndrome (Prevention and Control) Bill, 2014[vi]. The government also came up with the Electronic Health Records Standards for India. These helped in safeguarding the patient's financial information. All the existing laws regarding medical information privacy are scattered as they govern specific areas only. Looking into the changing scenario of digitalisation and storing health information

electronically it is important to have a comprehensive law that governs all aspects of health data privacy.

MEDICAL DATA PROTECTION LAWS IN OTHER COUNTRIES

Other countries also have certain data protection laws that govern the protection of health care data. Regarding data protection, the European Union has passed certain Data Protection Regulations for Privacy Impact Assessments relating to medical data[vii]. These regulations have provisions related to the consent of the patients for the use of medical information. Provision for explicit informed consent is mentioned as there is an unequal relationship between the patient and the doctor. Also unlike Indian laws, they have mentioned the right to be forgotten as when the clinical procedure is over patients may ask for deleting the information preventing any misuse. These provisions help in maintaining privacy. There are certain provisions which specify where the health information can be used. And General Data Protection Regulations are also implemented in the European Union prohibiting any organisation which processes or collects personal data from leaking it. In the United States also there are certain regulations that govern personal health care data. Digitalisation has increased the need for proper regulations as there are many threats to the privacy of patients. In the US the Health Insurance Portability and Accountability Act (HIPAA), 1996[viii] mentions certain provisions for the privacy of patient's health care information. The health care information was used by insurance companies for many purposes but infringed on the privacy of patients as medical data is sensitive in nature. The HIPAA provides provisions for the privacy of healthcare data and protection to the patients from their personal sensitive data to be misused. India does not have such protection laws for the health care sector. Apart from the EU and US other countries also have clear provisions for maintaining the privacy of patients. In Australia Privacy Act governs the collection of data with consent, transfer of data to any third party, securing the health data, etc. India has laws related to the health sector but those laws are not sufficient in the changing scenario. For better protection and ensuring the right to privacy in the health care sector, there is a need for more organised laws.

OVERVIEW OF DIGITAL INFORMATION SECURITY IN HEALTHCARE ACT (DISHA)

In India, there was a need for a complete law that could govern the health data of patients. As electronic health records are common and all the health-related data is stored electronically it is important to secure this data. Electronic recording of data has certain benefits but if this data storage is not regulated properly it could be misused. Already existing laws do not solve the purpose of maintaining the privacy of patients in all aspects. For fulfilling the need of providing security in the health sector the Ministry of Health and Welfare came up with the draft of the law which could help in removing the loopholes in the existing laws. India has a population in billions and to store and secure health data of such a large population is difficult. The Digital Information Security in Healthcare Act (DISHA) is a step for securing and maintaining health records of patients in the country. The main purpose of the draft is privacy, confidentiality, security and standardization of health data. The draft provides direction to the personal health care data of patients for the right use. It mentions the establishment of digital health authorities both centrally and at the state level. As India is a quasi-federal state it would be fruitful to establish governing authorities both at the central level as well as state level. At the centre, National eHealth Authority[ix] and at the state level State eHealth Authority[x] should be established to regulate the digital health care data. Interoperability of health data to some extent is also fulfilled by the provisions of the draft. It requires the establishment of Health Information Exchanges across the whole country which would help in improving the easy transfer of patient's health data[xi]. All the data could be stored in these exchanges in a standardized form providing a proper structure to the eHealth records in the country. As it not possible for a county like India with a huge population to maintain such a large quantity of digital data, there is central storage of data under the draft while ownership remains with the individual i.e. to the data belongs[xii]. Who should own the digital data was not mentioned earlier in any legislation, but the provisions of the draft specifically state that the patients should own their personal data and without their explicit consent this personal sensitive information cannot be used.[xiii] The exchanges would only be the custodian of personal health data. Many a time the health data is stored for a long period of time also after the clinical procedure. This stored data can be misused and manipulated. To avoid this draft provides provision for withdrawal of consent by the owner[xiv]. This also ensures the right to privacy which is an intrinsic part of the

right to life and liberty. Always it may be possible that after the withdrawal of consent health care may be refused to the individual. Taking care of this provision for not refusing any health care facilities to the individual if he refuses to give consent for the use of his personal sensitive health care information is mention in the draft. There are situations or purposes for which data may be need. For this draft explicitly mentions the purposes for which personal sensitive health information can be used. But this can also not be done without the consent of the owner. Even the government can use the data for some specific purpose only. There is provision for the access of health data for investigation purposes or if there is any order from the court.[xv] Health data is not only required to be processed by the clinical establishment and government only. Other service providers also use this data. The draft restricts any such use by entities other than clinical establishments for some limited purposes only. It also explicitly mentions that health data cannot be used for any other purpose which is not mentioned in the draft. Commercialisation of data is increasing day by data and this could infringe the right to privacy of an individual. Therefore the draft places a bar on the commercialisation of any health care data. The formulation of guidelines and standards for storage, transfer, processing of data should be the function of authorities set up at the state and central level. There should be proper check and balances to ensure that the norms are followed properly. This is to be done by the authorities and all these functions are mentioned in the draft. Also after all the laws and norms are explicitly mentioned there is a possibility for the breach of these laws. Therefore the draft also mentions the remedies for breach if any. There is serious punishment under the draft for any breach which includes imprisonment for five years and a fine upto five lakh rupees[xvi]. The draft also clearly mentions the types of breach in two categories i.e. breach and serious breach. Under breach, it involves punishment for any contraventions related to the collection of data or when data is not secured properly under the mentioned guidelines. And the serious breach is fraudulent activities involving commercial use of personal health care data. As the draft gives immense importance to the ownership of data by the patients, if there is any breach compensation may be granted to the owner from the person who is responsible for the breach. The said draft tries to overcome many loopholes of the already existing laws with respect to health care information.

LACUNAE UNDER DIGITAL INFORMATION SECURITY IN HEALTHCARE ACT

The draft of the act is a complete comprehensive law in the health care sector which could help in properly maintaining the personal sensitive health care record of patients and providing punishments in case of breach of privacy. But as we say there is always the other side, the draft has certain shortfalls also. People are getting highly dependent on technology; even health care facilities are available online through mobile applications. And there are many fitness wearables also used as people are getting more fitness freak day by day. All these applications and devices collect a huge amount of health care data which could be sensitive in nature. This health care data have certain benefits such as it can provide customised and better health care services to the patient. But on the other hand, this data is not secure and can be misused. The given draft also not allow using any such data as it secures and stores the data collected by the clinical establishments only. And these applications do not fall under the preview of clinical establishments[xvii]. Not only had this there certain other flaws also in the draft which need to be rectified for a proper law to come in function. The consent of the owner is the main point specified in the draft. But there is no mention of how this consent could be taken. There are many purposes for which there is need for health data and it could be time-consuming and expensive to seek consent for each and every patient for the use of their personal data for the purpose of research in the health sector. The artificial intelligence and many other technologies are dependent on data and the draft prohibits the access of data to such companies. The draft mentions and permits the use of personal health care data for research purpose with the consent of the patients but there is ambiguity in seeking such consent for the access of the data and how to store it. The draft is also not clear on the interoperability of data between different health information exchanges establish all over the country. It is unclear from the draft that where and under which exchange authority one should store its information. Nowadays outsourcing of health information is very common and this data that is outsourced is more prone to threats. The draft has not expressly deals with the outsourced health care data. As technology is getting advanced and the health care sector is also affected by the use of technology it is important to set up a law that also governs the technological advancements in the health care sector. For properly implementing the draft properly it is important that first there should be establishment of proper infrastructure.

RECOMMENDATIONS FOR CHANGES IN THE DRAFT

The said draft for the legislation related to storage, transfer, and privacy of data in the health sector is a better regulation than the existing laws. The development of technology in the health care sector needs the laws related to the privacy of the patient's health care data to be perfect. Therefore there is a need for the draft to be refined before implementing it. There should be clear provisions for seeking the consent of the patients i.e. the owner of the personal sensitive health care data. It is because when there would be proper provisions for the same time and money could be saved. It would also result in the introduction of better health policies by the government as access to data with the consent of the owner would be easy. The applications in mobile phones and fitness wearables that take information related to health care of the patients should also be governed under the Act. The use of such devices and applications is increasing day by day and it is important to secure and regulate this information also. To provide proper security and privacy to patients it is important to regulate data collected by such applications and devices. Also, outsourcing is increasing day by day and health information is outsourced at greater levels so it is prone to threats. Therefore proper provisions for securing outsourced data should be expressly mentioned under the draft. India needs better infrastructure for securing the health care data of the present population as well as the future population.

CONCLUSION

The right to privacy is an important right under the constitution of India, therefore it is important to secure this right of the citizens of the country in all possible way. The health sector in the country has not any proper legislation which could govern and protect the interest of the patients. The already existing also does not suffice the purpose of securing personal sensitive health care data. There was a need for some specific legislation for the concern matter. Also, the digitalisation of data in the health care sector makes it more important to secure the privacy of the patient's sensitive information. The draft for Digital Information Security in Healthcare Act helps to governing the health care sector to some extent with some flaws. Advancement in technology in the health care sector needs the government to protect the interest of the patients. However, the draft needs to be modified a little for better governance and in the changing scenario of health care in the country. With the development in the infrastructure for the said

draft, the future of health data could be secured and the patient's right to privacy could be preserved.

REFERENCES

[i] Rule 9(iv), The Clinical Establishments (Registration and Regulation) Act, 2010.
[ii]S.43 (A), the Information Technology Act, 2000.
[iii] S. 2 (c), Clinical Establishments (Registration and Regulation) Act, 2010
[iv] S. 2.2, the Clinical Establishment (Registration and Regulation Act, 2010)
[v] Rule 2(b), The Medical Termination of Pregnancy Regulations, 2003.
[vi] The Human Immunodeficiency Virus and Acquired Immune Deficiency Syndrome (Prevention and Control) Bill, 2014.
[vii]Article 33, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
[viii] Health Insurance Portability and Accountability Act, 1996.
[ix] S. 4, The Digital Information Security in Healthcare Act, 2018.
[x] S. 7, The Digital Information Security in Healthcare Act, 2018.
[xi] S. 19, The Digital Information Security in Healthcare Act, 2018.
[xii] S. 28, The Digital Information Security in Healthcare Act, 2018.
[xiii] S. 28(8) (b), The Digital Information Security in Healthcare Act, 2018.
[xiv] S. 28(8) (f), The Digital Information Security in Healthcare Act, 2018.
[xv] S. 29, The Digital Information Security in Healthcare Act, 2018.
[xvi] Chapter V, The Digital Information Security in Healthcare Act, 2018.
[xvii] Prosenjit Datta, *DISHA can serve as the model for data protection regulations and Privacy Act*, Business Today (01/06/2018), available at https://www.businesstoday.in/opinion/prosaic-view/disha-can-serve-as-the-model-for-data-protection-regulations-and-privacy-act/story/276019.html last seen on 13/11/2019.