Page 1227 - 1233 **DOI:** *https://doij.org/10.10000/IJLMH.112634*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 1

2022

Telemedicine and Data Privacy: An Issue Overlooked

AKSHAYA B[1] AND HARIVARDHANAN. R[2]

ABSTRACT

Telemedicine is the application of artificial intelligence when a health care provider and a patient are not in the specific physical location. This means that health-care services are delivered remotely through internet. Telemedicine services comprise the transmission of patient's health information in prescribed data formats for the purposes of diagnosis. It's worth noting, nevertheless, that using various telemedicine systems necessitates the processing of patient data. As a result, this problem should be assessed in terms of data security. Using telemedicine services will increase the link between health care providers and patients, but it should not have a negative impact on people's right to privacy. This must be viewed in the context of Indian legislation and the extent to which we have progressed towards the aim of data protection in numerous industries, such as health care..

I. INTRODUCTION

Indians are the second largest consumers of the Internet today. From shopping to sending marriage invitations online, we Indians have adopted the digitalization surprisingly very quick. Technologies are growing rapidly giving birth to newer innovations each passing day, to name a few, cars without a driver, an online currency (crypto-currency), fin-tech etc making our lives even more easier and comfortable. Everything is on the internet today but like everything comes with a cost, digitalization has gone a little far with it. We have all encountered privacy policies while entering into a website or a pop up asking to accept all the cookies. Most of us never go through those monotonous policies and just hit the "I agree" button. Same goes with social media applications.

Our Indian Constitution is a well structured, rigid rule of law determining the rights of Citizens. While it determines the fundamental and statutory rights, it does not specifically mention the kind of fundamental rights that it includes. From time to time judiciary has rightly intervened to uphold the rights of citizens. One such debatable right that has recently come under the purview of Article 21 of the Indian Constitution is "Right to Privacy". It took more than a

[1] Author is an Advocate at Tamil Nadu & Puducherry Bar Council, India.

[2] Author is an Advocate at Tamil Nadu & Puducherry Bar Council, India.

decade to finally recognize the right to privacy as fundamental right but the next most important consideration is the sources of such privacy breach which the legislation has to look into as early as possible. There can be multiple sources that aid breach of privacy. One such threat to privacy is offered by telemedicine which would be dealt in detail by us in this article. Information technologies have become an integral part of our daily lives because of the benefits that information technologies provide many processes in our business and personal lives are now based on the use of information technologies. The health sector is no exception. It is necessary to introduce a new type of information creation, storage, and circulation that would serve the needs of everyone involved in health care.

II. TELEMEDICINE

Telemedicine is also known as e-medicine. Telemedicine allows doctors to assess, diagnose, and treat patients without having to visit them face to face. Patients can communicate with doctors from the luxury of their own homes, without any need of standing or waiting in the queues, by just using their mobile phones or any suitable electronic device and visiting an e-medicine portal or any dedicated application for the same.

Telemedicine has no universally accepted definition. However, telemedicine is defined as the use of information and communication technologies to transfer medical information for the delivery of clinical and educational services.[3] The role of telemedicine has immensely grown recently in the times of COVID-19. While the country was facing a strict lockdown, people were agitated and obligated to stay at home and while the conditions were so people who were in need of medical help were rather scared to step out and the last thing anybody at that point wanted was to visit a hospital. Telemedicine grew in popularity because it allowed patients to be managed outside of hospital settings. It also allowed hospitals to allocate resources more efficiently and set aside space in their facilities for high-risk patients. It also enables people in low-resource areas, such as remote areas to receive medical assistance. Furthermore, it allows health-care providers to save some money by reducing the average length of appointments, and it allows them to save time and money on staff in the case of applications (apps). Nonetheless, there is a dangerous concern associated with this type of technology, and in order to comprehend it, we must examine a few additional principles.

III. DATA PRIVACY

The collection of information for a specific branch or topic is known as data. Whereas, privacy

[3] L. Hart, Norris 2002 "Low-Bandwidth, Low-Cost Telemedicine Consultations in Rural Family Practice", JABFP March-April 2002 Vol. 15 No. 2.

encompasses numerous characteristics such as non-disclosure of personal information, business secrets, personal relationships, private photographs and so on. Technically, if a person's personal text message is sent to another without their consent would be a breach of their Right to Privacy. We intentionally exchange data on a daily basis, and data is generated whenever we do something, booking a ticket or ordering a dinner online for example. When data is of great value, there is uncertainty about it, and a number of firms are tempted to use this approach to data. In today's technologically evolved society, data is the new currency. Despite all of the information available, the data's potential is yet unknown. New forms of technology are evolving, and new applications are being developed, which increases the value of such data.

India witnessed a lot of data privacy concerns recently which includes data of consumers from popular enterprises such as Air India, DOMINO’S, Big Basket, etc., making India the second biggest target of cyber crime in Asia.[4] The Pegasus case[5], for example, has demonstrated how Spywares can compromise a user's privacy and personal data. As a result, it is critical to analyse and implement a solid data privacy policy. Similarly, the Indian government has sparked a dispute by amending the Representation of the Peoples (RP) Act to require voters to provide their Aadhar numbers to electoral registration officers. While a section of people welcomed the move as it would restrict misuse of electoral rights but on the other hand, people are concerned about their data privacy. The fact to be considered here is not only the amount of data been collected by the government, online platforms, social media applications or any entity for that matter, but the potential of such data being collected. It is high time we recognize, as to how to identify and segregate our personal data based on its confidentiality. For example, we are reminded time and again by our banks and even by the government to not share our One Time Password (OTP) or the PIN numbers of our online payment apps (Fin-tech) with anybody. Hence, we are aware of the importance of this data and the seriousness it would pose if shared to a third party but what about the data we share online almost daily without knowing the repercussions like our gender, date of birth, photos and so on.

IV. TELEMEDICINE AND DATA PRIVACY

Now, let us look into the aspects with regard to how telemedicine and data privacy is an issue. Telemedicine is a broad term that refers to a variety of services. This issue should be considered from the standpoint of data protection because providing the aforementioned service involves

[4] IBM Security X-Force- https://www.moneycontrol.com/news/india/india-2nd-biggest-target-of-cyber-criminals-in-asia-pacific-in-2020-ibm-6569201.html.

[5] Manohar Lal Sharma vs Union Of India (2021) SCC Online SC 985

the transmission of personal data about the patient's health via text messages, sound, images, and other forms of data for the prevention, diagnosis, treatment, and follow-up of the patient. Greenbone Networks, a German security firm, has identified many health data breaches and leaks in India. A breach of patient data from India, including X-ray images, names, diseases, and treating physicians, was reported in February 2020, pointing flaws in the confidentiality and data protection system.[6]

While so, the right to privacy was described in US by Justice Brandeis in Olmstead v. United States[7] , as "right to be let alone... the most comprehensive of rights and the right most valued by civilised men". This has been recognized under our Constitution by the Supreme Court in Kharak Singh vs. State of Uttar Pradesh.[8], Gobind vs. State of Madhya Pradesh[9] , R.Rajagopal vs. State of Tamil Nadu[10], District Registrar and Collector vs. Canara Bank[11] , and recently in Justice K.S.Puttaswamy(Retd.) vs. Union Of India[12] where Right to privacy was recognized as a fundamental right. It is important to recognise the threat to privacy through online platforms especially Technologies like telemedicine where people share their health information like blood tests, X rays, MRI reports etc in addition to their personal data in a more vulnerable state without realising the implications of such data if leaked. Even though we have regulations regarding Doctor patient confidentiality, we have no laws regarding the protection of these data.

V. DATA SECURITY LEGISLATION AND ITS FEATURES

There are no clear or stringent rules for data protection in India which is resulting in an alarming rise of cybercrime. Data protection exists to safeguard an individual's personal information. As of present, there is no explicit data protection law or regulation in India. However, there are certain statutes and acts that contain provisions that address this issue, including the Indian Constitution[13], Copyrights Act[14], Information Technology Act[15], IPC[16] etc. Yet, all of these statutes do not deal with data privacy nor does it deal with telemedicine specifically.

Recently, the final report on the "Data Protection Bill" was approved by the Joint Committee

[6] Chandrashekar A. - German firm finds one million files of Indian patients leaked. via The Economic Times. 2020.

[7] 277 US 438 (1928)

[8] (1964) 1 SCR 332

[9] (1975) 2 SCC 148

[10] (1994) 6 SCC 632

[11] (2005) 1 SCC 496

[12] (2017) 10 SCC 1, AIR 2017 SC 4161.

[13] Article 21- Right to life under The Constitution of India, 1950.

[14] Section 63B of Indian Copyrights Act,1957.

[15] Section 43A, 72 and 72A of Information Technology Act,2000.

[16] Section 403 of Indian Penal Code,1860.

of Parliament (JCP). Data protection while safeguarding individual privacy is a pressing need of the hour. The passage of the data protection bill is a step in the right direction. The bill was previously known as the Personal Data Protection Bill of 2019, but the JCP has proposed changing the name because it would now include rules on non-personal data.[17] It will be known as the Data Protection Bill, 2021, and will become the Data Protection Act if it is passed.

After the Puttaswamy Judgment in 2018, the Personal Data Protection Bill of 2019 was one of the most anticipated bills of the year. The bill include a number of provisions, including the creation of an Indian Data Protection Authority to secure personal data, prohibit misuse of personal data, safeguard individual’s interests, and raise knowledge about data protection and policy. The bill also allows for the transfer of data outside of India, but only with the individual's express consent. Data collection should be done for a defined purpose, and the information gathered should be limited to that purpose with the individual's explicit consent. The bill defines sensitive personal data, such as financial data, biometric data, caste, political beliefs, and so on, and prohibits their acquisition unless consent is obtained. Data Fiduciaries, as defined by the Act, are entities or individuals who decide on the purpose of processing personal data, which could include the government. The standards that such fiduciary must adhere to, have also been established in the bill.

The present legislation dealing with data privacy issues in India are the Information and Technology Act, 2000 and its Rules, as well as sectoral regulator specific circulars and guidelines, such as those issued by the Reserve Bank of India (RBI) and the Insurance Regulatory and Development Authority. Speaking of Information technology, it would be imminent to know about The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the SPDI Rules) govern the security of personal data gathered by corporate. It defines 'personal information' as any information on a natural person that, when combined with other information held by the corporate, can be used to identify that person. The SPDI Rules demand corporations to establish an easily accessible privacy policy that explains what types of personal information they collect, why they gather it, how they use it, who they share it with, and what acceptable security mechanisms they have in place.

Similarly, with regard to Telemedicine, some rules were created in collaboration with the NITI

[17] Non- Personal Data- In its most basic form, non-personal data is any set of data which does not contain personally identifiable information. This in essence means that no individual or living person can be identified by looking at such data. Eg- Name, Age, Gender etc- What is Non- Personal Data, Article from The Indian Express (dt. 27.07.2020).

Aayog (National Institution for Transforming India) and the Board of Governors of the Medical Council of India, India's former medical education regulator, in order to address a fundamental gap, the lack of legislation and a framework for ethical telemedicine practise.[18] The Indian government has established Telemedicine Practice Guidelines to allow Registered Medical Practitioners (RMPs) to provide health care services utilising a variety of telecommunication and digital communication technologies. The Indian Medical Council Act, 1956 defines RMP as "a person who is enrolled in the state registry or the national register."

VI. Recommendations

With data protection bill, awaiting the approval it need some alterations according to us.

- Firstly, Data Protection Bill is silent on Telemedicine and data privacy issues. With telemedicine being the most used platform during the pandemic, it needs an urgent attention with regard to privacy legislation. If a person is infected with COVID-19 he cannot go out and risk infecting others. In this situation, people will almost certainly be obliged to adopt whatever technology their healthcare professional chooses, both for their own sake and the benefit of the general public and in such situation people share their data vulnerably online.
- There is a need for more complex regulation and guidance for the use of such technologies in the health sector, which can be achieved by ensuring that there is a defined structure and standards for telemedicine. Compliance with current safeguards, such as those contained in health standards and data protection regulations might be a part of these frameworks. These comprehensive e-health and specific strategies and frameworks, as well as any necessary legislation regarding telemedicine, will help ensure that there is a framework in place to guide and oversee the implementation of such digital tools in the health sector, as well as define the roles and responsibilities of the various factors involved in the said ecosystem.
- Generally the burden of maintaining records of all doctor-patient communications lies on doctors. The rules currently do not stipulate a time limit for storing the data or any restrictions on how that data might be used in the future. The requirements merely stipulate that the practitioner must be aware of and follow all applicable data protection and privacy laws. Therefore, the legislature must look into this issue while framing the act and also must include the aforementioned time limit to store these data.
- While the average consumer isn't used to sifting through privacy rules, the Notification demands them to do so. Privacy policies, on the other hand, are frequently written in ambiguous

[18] S. Saxena, K. Srivastava, R. Dilbagi, and A. Saxena Madhya Pradesh's experience with telemedicine units for COVID-19- Community Health in Indian Jurisprudence. 2020;32(2 Special):277–280. https://doi.org/10.47203/IJCH.2020.v32i02SUPP.021.

language and are rarely read. Even in this sensitive moment, it will be shocking if all privacy rules are explicit and specific about how they handle information. Furthermore, users have no control over their data and are unable to negotiate privacy arrangements with telecom providers prior to using their platforms. Rather, these businesses have a "take it or leave it" attitude. Consumers do not benefit from the business incentives introduced by the pandemic emergency. It provides a significant benefit to commercial enterprises and improves their marketing capabilities. As a result, there is a considerable possibility of economic exploitation. Hence, the privacy policies must be negotiable and user friendly and must aim at providing safe service to the consumers.

VII. Conclusions

Doctors, health experts, and federal authorities are now only realising how difficult it is to keep records safe. According to us, to make portable data more safe, healthcare professionals can use cloud storage, authentication mechanisms like strong passwords and encryption. The use of a two-factor authentication system that includes security tokens and a password can assist secure data. To safeguard data integrity, security measures such as firewalls, antivirus software, and intrusion detection software must be used. Patient privacy and confidentiality are protected by specific policies and procedures. The institution must choose a security officer to collaborate with a team of health IT professionals. Random audits should be undertaken on a periodic basis to assure that hospital policies are followed. Audit trails can be used to track all system activity. This contains complete content, length, and user listings, as well as the generation of date and time for entries and logs of any data updates. Whenever anyone gains unauthorised access to a medical record, the system can provide information including the person's name, the time and date of the review, the screens accessed, and the length of the review. This data can be used to determine if the access was unintentional or a planned, unlawful view. As of now India has not witnessed any serious health data leak incidents nor has it been taken seriously by the Judiciary or the Government yet. It is the need of the hour that we focus our attention towards telemedicine and the underlying threats. As already mentioned, there are no specific laws that deal with telemedicine but with a never ending pandemic, it is necessary for the legislative to frame a suitable law regarding the data privacy concerns of telemedicine. As they say, prevention is better than cure, it is high time the judiciary and the legislative start taking this issue seriously and prevent a larger obstacle in the future by providing a safe and healthy online medical experience.

*****