The Indispensable Trade-off: A Confluence of Privacy and Data Sharing in Assuaging a Global Health Emergency

Garima Khanna
Student,
Dr. R.M.L.National Law University, Lucknow.
Email: garmiak1000@gmail.com,

Kunwar Siddhant Pal
Student,
Dr. R.M.L.National Law University, Lucknow.
Email: siddhant.alp1@gmail.com

Reference to this paper should be made as follows:

Garima Khanna, Kunwar Siddhant Pal

The Indispensable Trade-off: A Confluence of Privacy and Data Sharing...

Journal Global Values, Vol. XII, No.I
Article No.18,
pp. 140- 153
https://anubooks.com/jgv-vol-xi-no-1-jan-june-2021/

https://doi.org/10.31995/jgv.2021.v12i01.018

Abstract

While combatting the nonpareil crisis with smattering knowledge the Kerala government was under fire for transferring the medical data of its citizens to wane the incessant death rate in the state. While the state was believed to be in the interest of its people, the furor of Kerala forced the government to retract its decision. While the authors believe that due to these unprecedented times it is pertinent that the civilians should relinquish their right to privacy to a certain degree, they are cognizant of the blemishes that prevail in the health infrastructure of India. With a few bulwarks, however, the authors feel that sharing medical data will be an advent in routing the virus that has upended the entire world.

Introduction

Kerala government had entered into a contract with a US-based IT firm Sprinklr, wherein the data of suspected and actual patients of COVID-19 would be collected using government machinery and uploaded to the foreign firm's web server daily. The data includes details of their symptoms and underlying health conditions, compiled by workers at the grass-roots level using a tool developed by Sprinklr[1]. The IT company, in turn, would provide actual data to the state machinery after analysis, for better understanding and treatment of the pandemic. The government, however, after much criticism decided to retractfrom the deal due to privacy issues[2].

This deal, however, sheds light on a major conflict between the laws of India. If there is a conflict between the privacy rights of an individual and the collective good of mankind, what should be given preference? The authors in this paper discuss and try to reason out as to why sharing such medical data is essential at a time of global crisis. The authors in this paper explore the bounds of privacy and the subsequent trade-off which must be met between individual rights and the larger collective good in face of a global health emergency.

The major conflict-Exigency v Fundamental Right of Privacy and Inadequate infrastructure.

It is well settled that, the right to privacy comes under Article 21 of the Constitution after the Puttaswamy judgment[3]. The judgment further clarifies that a constitutional right to privacy can be defined in both negative and positive terms,

1.To protect the individual from unwanted intrusion into their private life, including sexuality, religion, political affiliation, etc. (the negative freedom)

2.To oblige the state to adopt suitable measures to protect an individual's privacy, by removing obstacles to it (the positive freedom)

However, we must realize that no right is absolute and there have to be certain restrictions. Justice Nariman has held in paragraph 60 of his judgment that statutory restrictions on privacy would prevail if it is found that the 'social or public interest and the reasonableness of the restrictions outweigh the particular aspect of privacy claimed. The court furthers discussed in detail, data protection or informational privacy and came to a conclusion that the state has the authority to breach informational privacy on three-fold requirements:

1.Existence of law to justify an encroachment on privacy; and

2.The requirement of a need, in terms of a legitimate state aim, ensures that the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, a guarantee against arbitrary state action.

[The legitimate aims of the state comprise of protecting national security, preventing and investigating crime, encouraging innovation along with the spread of knowledge, and preventing the dissipation of social welfare benefits]; and

3. The means which are adopted by the legislature are proportional to the object and needs to be sought to be fulfilled by the law. Proportionality is an essential facet of the guarantee against arbitrary state action because it ensures that the nature and quality of the encroachment on the right are not disproportionate to the purpose of the law.

As of now, there is no law in black and white to deal with the particular issue. However, there are several treaties and conventions ratified by India which warrant the encroachment of privacy by the state.

Also, it would be moot to argue if the state has a legitimate aim in sharing the data. The present situation dictates the state to take every possible measure to mitigate the severity of the situation. The Kerala government believes that sharing such data would help the nation and such times call for a collective effort on part of the entire world to fight the pandemic.

The means adopted by the state are well in proportion to the object that needs to be sought to be fulfilled. COVID-19 is a very peculiar situation and has to be fought in every possible manner. If the government believes that the IT company can help in analyzing and improve the chances of combating the life-threatening disease, collection and transferring of such data should not be considered to be out of proportion to the object sought to be achieved by the state.

In Union for Civil Liberties (PUCL) v Union of India[4] , the Supreme Court observed that when there is a competition between the right to privacy of an individual and the right to information of the citizens, the former right has to be subordinated to the latter right as it serves the larger public interest.

In Sharda v Dharmpal[5], the Supreme Court said that though the right to personal liberty has been read into Article 21, it cannot be treated as an absolute right. To enable the court to arrive at a just conclusion a person could be subjected to a test even though it would invade his right to privacy. It concluded that one has to maintain a balance between the rights of a citizen and the right to privacy.

Personal Data Protection Bill, 2019[6], states that there are certain exceptions provided under which Personal Data can be processed if required by the State for providing benefits to the individual, legal proceedings, to respond to a medical emergency.

Section 5(2) of the IT Act[7] states that a body corporate or any person on its

behalf can collect sensitive personal data or information if:

1.The information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf, and

2. The collection of sensitive personal data or information is considered necessary for that purpose.

Storing data digitally is also termed an Electronic Health Record (EHR). It is a collection of various medical records that get generated during any clinical encounter or event. With the rise of self-care and homecare devices and systems, nowadays meaningful healthcare data get generated 24x7 and also have long-term clinical relevance. The purpose of collecting medical records, as much as possible, are manifold – better and evidence-based care, increasingly accurate and faster diagnosis that translates into better treatment at lower costs of care, avoid repeating unnecessary investigations, robust analytics including predictive analytics to support personalized care, improved health policy decisions based on a better understanding of the underlying issues, etc., all translating into improved personal and public health.[8]

The shift from paper records to EMRs is the future of the medical industry, it's a global phenomenon. Such records will not only have benefits like reduction in costs for hospitals, facilitation of review of medical errors, improvement in the quality of care with greater transparency about the patients for healthcare providers and efficiency in the healthcare system but will also contribute to their growth, the ability to mine and process large volumes of medical data that can be invaluable for research and analysis. It can further be used to predict epidemics, prevent disease before it occurs, personalize diagnostics, improve the efficiency of drugs.[9]

Article 4 of the ICCPR[10], which declares the right to privacy as an essential right, states that in time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, the States Parties to the present Covenant may take measures derogating from their obligations under the present Convention.

The natural and customary meaning of "public emergency threatening the life of the nation" is clear and refers to "an exceptional situation of crisis or emergency which affects the whole population and constitutes a threat to the organized life of the community of which the State is composed"[11].

Data protection rules such as General Data Protection Regulation do not hinder measures taken in the fight against the coronavirus pandemic.[12]

Article 9(2)(i) of the GDPR[13] explicitly allows the processing of sensitive personal data (including genetic data, biometric data, and data concerning health) if

it is "necessary for reasons of public interest in the area of public health." Recitals 46, 52, 53, and 54 also explicitly acknowledge the need to sometimes process special categories of personal data for reasons of public interest in the area of public health. Furthermore, article 9(2)(j) sets out a scientific research exemption for the processing of sensitive personal data, which could occur without consent if subject to appropriate safeguards,

The duty to share information to support safe and effective healthcare may be as important as the duty to protect confidentiality.[14]Many patients lack awareness and understanding about the potential uses of health information, the protections in place, and how sharing information can benefit themselves and others.[15]

Researchers can help to increase public understanding about the potential benefits of research and the potential dangers in not learning from the data by engaging in public education and debate.[16]

Rothman asserted that "the real roadblock for epidemiologic research" is the difficulty in addressing these privacy concerns adequately without compromising the quality of the research, and he stressed the value to individuals and society of expanding knowledge in medicine and public health.[17]

Nathan Hershey, pointed out, how to strike a balance between the medical and public health benefits that accrue to individuals and society from the results of epidemiological research versus maintenance of the privacy of medical records, which is "an important and increasingly recognized value in our society.[18]

Gilbert Beebe, the eminent radiation epidemiologist, writing around the same time as Rothman, also stated that to cope with the increasing demands of our society for prevention, treatment, and compensation, we need more, precise, information on health hazards; yet we have not been willing to face up to the implications of these needs. Satisfying them will require better planning and integration of existing information systems, additional funds, and some trifling sacrifice of personal privacy.[19]

At the same time as society is being challenged daily by new and grave threats to public health, research efforts are being constrained by what seems to us to be excessive limitations on access to data requested for the explicit purpose of improving public health.[20]

Health databases and biobanks have also previously been framed as solidarity-based endeavors, and solidarity-based governance models have been proposed to reflect the prosocial motivation many people have toward such resources, which at the same time avoid some of the burdens of the usual restrictive, autonomy-based governance models.[21]

On the surface, requiring people's consent before being able to store and use personal information about their mental and physical health, seems difficult to argue against. However, the situation is incredibly complex, especially when it comes to medical research that relies so heavily on data-rich sources such as disease registries. Without access to data sets from registries and health records, large-scale, population-based research would not be possible. Huge medical advances have been made through using such data.[22]

Health care information also has particular relevance apart from an individual's health. Taken in the aggregate over many people, long-term large-scale population studies allow the discovery of statistical correlations between environmental factors and disease and are also used to help assess the efficacy of treatments, to determine the overall costs of particular kinds of treatment regimes, and to conduct epidemiological research that can generate insight into the genesis, development, and spread of disease.[23]

Article 8(2) ECHR[24] could provide an answer to the question of permissible limits on the right to privacy. In the context of the challenges posed by the pandemic, it is important to state in this article that the factors which may justify the state limiting the right to privacy include public safety, protection of health and protection of the rights and freedoms of others. It is, therefore, necessary in each case to balance the relationship between the good being protected and the good being sacrificed.[25]

Moreover, Article 15 ECHR[26] claims that in time of war or other public emergency threatening the life of the nation any state may take measures derogating from its obligations under a Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law. It ultimately requires a healthy and congenial interrelationship between the social good and individual liberty.

Keeping in mind the above-stated conventions and observations of renowned scientists of several other nations, it can be concluded said that a COVID-19 pandemic is an unprecedented event that has resulted in numerous deaths and this rate is constantly rising, causing major concerns to the safety of people of the nation. If the government is sharing such data, it is because it is the need of the hour and the world needs to take a collective step to eradicate the disease.

On the other side of the spectrum lies the major concern of the momentous nature of privacy and the inadequacy of the current legal framework.

Privacy refers to the ability to control who knows what about us, the view of

privacy as an opportunity to limit another's access to personal data, regardless of whether it is a matter of another person or an institution[27], protecting personal data, personal space and personal choices.[28] Part of the views on privacy focuses on the control over a person's information as the ability to define the individual based on when, where and to what extent the information related to a said individual is shared with others.[29] One of the more contemporary definitions of privacy is William Parent's [30]definition according to which privacy is the condition of not having undocumented information on an individual, known to or possessed by others.

The term "privacy" has been described as "the rightful claim of the individual to determine the extent to which he wishes to share of himself with others and his control over the time, place and circumstances to communicate with others. It means his right to withdraw or to participate as he sees fit. It also means the individual's right to control the dissemination of information about himself; it is his possession."[31] According to the laws of various nations, Highly Sensitive data includes personal information that can lead to identity theft. It also includes any health information that reveals an individual's health condition and/or medical history[32].

Medical data fall into the category of sensitive personal data, so their processing is prohibited. Data on the health of the citizens, must not be disclosed publicly.[33] Article 4 of the Regulation (EU) 2016/679 of the European Parliament and the council specifically mentions that the Health Information of an individual is highly sensitive and is subjected to certain regulations.[34]

'Health and medical information (including medical records, prescription histories, patient data, surgical records, and so on) are one of the most obvious of those types of information that have long been considered to be personal and deserving of privacy protection.[35]' The Hon'ble Supreme court in the case of Selvi v. State of Karnataka[36] observed that a medical examination cannot justify the dilution of constitutional rights such as the right to privacy which denies the state of the defense of medical use of data.

In Air India Ltd. v Cochin International Airport Ltd[37] and Ramana Dayaram Shetty v International Airport Authority of India and Ors[38], the Hon'ble SC observed that there is a duty imposed on the state to act reasonably while obtaining consent from individuals for the collection of information which falls under the protection envisaged under the right to privacy, without regard to, under what capacity function is being exercised by the state.

The International Covenant on Civil and Political Rights[39] directs that the gathering and holding of personal information on computers, data banks and

other devices, whether by public authorities or private individuals or bodies, must be regulated by law. To have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data ûles, and for what purposes.[40]. The 35th International Conference observed a similar principle[41].

According to the EU Charter of Fundamental Rights, everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law.[42]

Privacy is the major concern of the general public whilst giving information to the government which itself lacks a proper framework for storing such information and transferring such data to a company situated overseas.

Besides the fact that the government lacks a legal basis to store the information of citizens another thing to keep in mind is the technological aspect. Privacy of an individual is a major concern and transferring of such medical records to another entity amounts to infringement of such right.

Section 43(a)[43] and Section 72[44] of the Information Technology Act provide the broad framework for the protection of personal information and its privacy in India.

Section 43(a) outlines the standards that need to be followed by an entity that collects or stores or in any way deals with sensitive information such as passwords, financial information, health conditions, sexual orientation, medical records and biometric records – directs corporates to take reasonable steps to protect sensitive personal data of individuals 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."

The major issue that lies in front of the government is that majority of India's population cannot afford private healthcare, therefore, public medical services and hospitals are undoubtedly used more often. There is a lack of remedies in case public hospitals or non-profitable organizations do not maintain reasonable security practices, thus a large volume of personal information is left vulnerable and unaccountable for.

The primary law that establishes the US legal framework for health information, HIPAA gives patients substantial control over their information.

The new EU General Data Protection Regulation requires member states to protect medical data from human and technical failures and provides detailed grounds for processing such data and its use for secondary purposes like research and development.

Presently, the framework that envisages EMRs in India is the Electronic Health Record Standards released by the Ministry of Health and Family Welfare[45]. This document chalks down the international technical, administrative and physical standards for data protection concerning health records specifically.

However, even these standards are not impeccable and have their shortcomings as there is an unclear scope of coverage, lack of clarity in terms of timelines for accessing patient's records, and ambiguity in defining the scope of 'personal health information.'

A health record system must meet architectural requirements and functional specifications to remain faithful to the needs of service delivery, be clinically valid and reliable, meet legal and ethical requirements, and support good medical practices.

While EMRs will provide the government with wider access to medical information enabling them to improvise and upgrade the healthcare system and public policy devised to aid the citizens, the legal framework supporting such a governance initiative, specifically relating to data security and privacy, remains inadequate.

Therefore, there is no clear framework governing electronic medical records and how they are collected and used, and nor are their remedies for data breaches due to the negligence of hospitals.

The way around it.

Inter armaenim silent lēgēs "In times of war, the law falls silent." COVID-19 is a first-time event experienced by the entire world. It has affected the global economy and has brought the entire world to a standstill. Extraordinary situations require extraordinary measures and if sharing of medical data will overall benefit the world, the people may consider keeping aside certain privacy concerns.

However, the government needs to realize that India is way behind the West when it comes to data safety and protection and infringement of privacy is a genuine concern of many people. A solution to this paradox is the anonymization of data.

When the question of privacy regarding medical records was placed before the National Law University, it submitted a draft that suggested that such data should be de-linked from a person before it uploaded on a digital platform.[46] "If the data is legally owned by the person to whom it belongs, one concern is that data once de-identified should also be available to the government and researchers," said an expert

committee member. If the owner of the data is not in the favour of sharing any personal information, anonymization of the data will destroy the identifiable pieces of information permanently at the source.

Data anonymization is a computing standard in which sensitive medical information contained in electronic health records (EHR) can be anonymized so that unauthorized users are unable to read the actual content since it is no longer in its original state. There are two types of data de-identification and they are the statistical method which makes the EHR disconnected to the individual that has been rendered anonymous by stripping out any information that would allow people to determine an individual's identity[47].

Lawrence E. Hunter a Professor and Director of the Centre for Computational Pharmacology at the University of Colorado School of Medicine attempted to present methods to anonymize data that would help the scientist to share data, the clinician to use that data, and ultimately, the patient to benefit from the data in terms of new treatments.[48]

Fear of data sharing needs to subside when we see the benefits that interoperability of our medical records brings us and we benefit both personally and as a community.

Conclusion

India should take note of the best practices evolved by countries with more mature governance systems for electronic health and medical records. Considering the extremely sensitive nature of medical information and the adverse impact a breach can have on an individual's life, the government must fast-track the Healthcare Data Privacy and Security Act to cover all hospitals and ensure that the regulator is prompt in addressing instances of negligent security and misuse of personal information.

The law would allow anonymized health data, which cannot be traced to individuals, to be used for specified public health purposes, such as early detection and rapid response public health emergencies such as bioterror events and infectious disease outbreaks.

In recognition of the serious privacy and security concerns over the uses and misuses of digital health data, the proposed law would completely prohibit the use of digital health data for 'commercial purposes, whether in an identifiable or anonymized form. This would mean that insurance companies, employers, human resource consultants and pharmaceutical companies would not be allowed to access or use health data.[49]

Privacy is without a doubt a major concern while dealing with the transfer of medical data. However, at a time like the present, we need to keep that concern at bay especially after such data has been delinked and can be used to save the state from the harrowing implications of the uncontrolled epidemic.

The medical data of citizens at this point is critical for policymaking as well. For example, for policy-making on HIV treatment, a policy-maker needs to know how many individuals are HIV positive. The entire world is wet behind the ears to combat the deadly disease as there is still neither a cure nor a vaccine. All we have available at our disposal are hit and trial methods and for this, the government needs to know the underlying conditions of the people for coming up with better policies as well as treatments.

The government must protect its citizens from such pestilence and try its best to bring back the state to normalcy. Sharing of data is just a part of that effort on part of the government. It is legitimate why the citizens of Kerala lack trust in the government's idea of sharing the data to an overseas private entity but before having such concerns a bigger moral question comes into play- The benefit of the entire state. Sharing such medical data after anonymization will not only help the state but the world at large.

References

1 Vishnu Varma, *Explained: What is the Sprinklr row Kerala govt's Covid-19 response is embroiled in?*, April 21, 2020,https://indianexpress.com/article/explained/what-is-the-sprinklr-row-kerala-govts-covid-19-response-6371205/ (Last visited on July 19, 2020).

2 Jamon Jacob, Kerala backs out of Sprinklr deal, cancels controversial pact over privacy issues, May 21, 2020,https://www.indiatoday.in/india/story/kerala-sprinklr-deal-covid-19-pinarayi-vijayan-high-court-1680484-2020-05-21 (Last visited on July 20, 2020).

3 K S Puttaswamy v. Union of India, (2018) 1 SCC 809.

4 Union for Civil Liberties v. Union of India, AIR 1997 SC 568.

5 Sharda v.Dharmpal, (2003) 4 SCC 493.

6 The Personal Data Protection Bill, 2019, Bill No. 373 of 2019[7] Information Technology Act, 2000, s 5(2).

8 Ministry of health and family welfare, *Electronic Health Standard (EHR) 2016* , December 30, 2016, available at https://main.mohfw.gov.in/sites/default/files/17739294021483341357.pdf

(last visited on July 23, 2020).

[9] Yang S, Santillana M, Brownstein JS, Gray J, Richardson S, Kou SC, *Using electronic health records and Internet search information for accurate influenza forecasting*, 17 BMC Infect Dis. 332 (2017).

[10] International Covenant on Civil and Political Rights, 16 December 1966, UNTS, vol. 999, p. 171.

[11] Lawless v Ireland, (No 3) (1961) 1 EHRR 15.

[12] European Data Protection Board, *Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak,* March 16 , 2020, <www.edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en>(Last visited on 15 June, 2020).

[13] EU General Data Protection Regulation (GDPR), art 9(2)(i).

[14] Dame Fiona Caldicott, Review of Data Security Consent and Opt-Outs33 (2016).

[15] Hill EM et al,Let's get the best quality research we can, 23 (2013).

[16] Lancet Res Med, *Data protection: balancing personal privacy and public health*,2016, www.thelancet.com/journals/lanres/article/PIIS2213-2600(15)00514-7/fulltext (Last visited on July 23, 2020).

[17] Rothman, *The epidemiologist's lament,*72 AJPH 1309,1311 (1981).

[18] Hershey, *Putting the lamentations of epidemiologists in perspective,* 72AJPH 1155, 1157 (1982).

[19] BeebeGW, Long-*term follow-up is a problem,* 73AJPH 245, 246 (1983).

[20] Ann Aschengrau et al, Essentials of Epidemiology in Public Health 324 (2018).

[21] Katharine A Wallis, *Research using electronic health records: Balancing confidentiality and the public good,*10 JPHC 288, 291 (2018).

[22] Lancet Res Med, Data protection: balancing personal privacy and public health, 2016, www.thelancet.com/journals/lanres/article/PIIS2213-2600(15)00514-7/fulltext (Last visited on July 23, 2020).

[23] National Research Council, Engaging Privacy and Information Technology in a Digital Age90 (2016)

[24] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, art 8(2).

[25] Dr. Olga Hałub-Kowalczyk, *Redefining the Right to Privacy in the Age of the COVID-19 Pandemic*, April 2, 2020,available at www.iconnectblog.com/2020/04/redefining-the-right-to-privacy-in-the-age-of-the-covid-19-pandemic/ (Last visited on July 24, 2020)

[26] European Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe, as amended by Protocols Nos. 11 and 14, art 15.

[27] James Rachels, *Why Privacy Is Important*, 4 Philosophy and Public Affairs 323,333 (1975).

[28] T Anita Allen et al, *Unpopular Privacy: what must we hide?,* 15Ethics Inf Technol 63,67 (2013).

[29] Alan F Westin, *PRIVACY AND FREEDOM,* 22American Bar Association 101,106 (1969).

[30] Parent, W A,*Privacy,Morality, and the Law. 12 Philosophy & Public Affairs 269,288* (1983).

[31] Adam Carlyle Breckenridge, *The Right to Privacy* 32 University of Nebraska Press 152 (1970).

[32] Virginia Code, s 18.2.

[33] Elena Stojanovska, Jovana Ananievska, Privacy, information and public interest: The right to privacy versus the public's right to know 205-06 (1st edn 2015).

[34] European commission, *EU Data protection rules,* European commission , 2019,<https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds processing-data/sensitive-data/what-personal-data-considered-sensitive_en>(Last visited on June 14, 2020).

[35] Lynette I Millett et al, *Engaging Privacy and Information Technology in a Digital Age* (2nd edn, National Academies Press 2007).

[36] Elena Stojanovska, Jovana Ananievska, Privacy, information and public interest: The right to privacy versus the public's right to know 205-06 (1st edn 2015).

[37] Air India v. Cochin International Airport, (2000) 2 SCC 617.

[38] Ramana Dayaram Shetty v. International Airport Authority of India, (1979) 3 SCC 489.

[39] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, UNTS, vol. 999, p. **171.**

[40] ICCPR,*General Comment No. 16, Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honor and reputation)*, Refworld1988, available at https://www.refworld.org/docid/453883f922.html (last visit July 26, 2020).

[41] European Union Agency for Fundamental rights, *35th international conference of data protection and privacy commissioners: Data protection, privacy and new technologies*, September 26, 2013, available at https://fra.europa.eu/en/event/2013/35th-international-conference-data-protection-and-privacy-commissioners (last visited on July 26, 2020).

[42] Markandeya v. State of A.P, (1989) 3 SCC 191.

[43] Information Technology Act 2000, sec. 43(a).

[44] Information Technology Act 2000, sec. 72.

[45] Ministry of health and family welfare, *Electronic Health Standard (EHR) 2016* , December 30, 2016, available at https://main.mohfw.gov.in/sites/default/files/17739294021483341357.pdf(last visited on July 23, 2020).

[46] Anumeha Yadav, *Who will own your data when your electronic health records are linked to Aadhaar*? April 5, 2017,available at https://scroll.in/pulse/833190/aadhaar-in-health-records-legal-experts-and-government-divided-over-who-will-own-data (last visited on July 19, 2020).

[47] Kushida CA, Nichols DA, Jadrnicek R, Miller R, Walsh JK, Griffin K.,*Strategies for de-identification and anonymization of electronic health record data for use in multicenter research studies*, 50 *Med Care*. 226(2012);

[48] Hunter LE, Hopfer C, Terry SF, Coors ME. *Reporting actionable research results: shared secrets can save lives*, 4 SciTransl Med. 143 (2012).

[49] Madhur Singh, India proposes a law to give Indians Complete control of their digital health data, May 31, 2018, available at https://www.indiaspend.com/india-proposes-law-to-give-indians-complete-control-of-their-digital-data-58073/ (last visited on July 25, 2020).