॥न्यायस्तत्र प्रमाणं स्यात्॥

NATIONAL LAW UNIVERSITY DELHI

Prof. (Dr.) Ranbir Singh
Vice-Chancellor

September 21, 2020

Dr. Indu Bhushan
Chief Executive Officer
National Health Authority
Government of India
9th Floor, Tower - I, Jeevan Bharati Building,
Connaught Place, New Delhi - 110001

Subject: Submission of Comments on the Health Data Management Policy for National Digital Health Mission

Dear Dr. Bhushan,

The National Law University Delhi is a publicly funded university established by the government of the National Capital Territory of Delhi on the initiative of the High Court of Delhi, via Act No.1 of 2008 of National Capital Territory of Delhi. The Chief Justice of India is a Visitor to the University and the Chair of the Governing Council. The Chief Justice of High Court of Delhi is the Chancellor of the University.

The Centre for Communication Governance (CCG) was established by the University in 2013 to ensure that Indian legal education establishments engage more meaningfully with information law and policy, and contribute to improved governance and policymaking. CCG is the only academic research Centre dedicated to working on information law and policy in India.

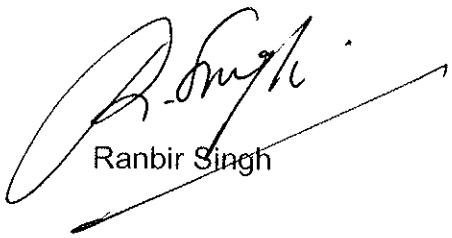
We welcome the opportunity to comment on the Draft Health Data Management Policy for National Digital Health Mission and commend the NDHM under your leadership for adopting a public and consultative approach to the whole process.

As part of our work, and given how critical it is to provide lawmakers with useful material, we have drafted comments to the Draft Health Data Management Policy which are enclosed herewith.

We hope that these comments are of assistance to the NDHM in formulating its final policy and recommendations on the issue of utmost importance.

We will be happy to find any additional material and my colleagues Ms. Smitha Krishna Prasad (smitha.prasad@nludelhi.ac.in; +91-9980175343) and Mr. Sarvjeet Singh (sarvjeet.singh@nludelhi.ac.in; +91-9990232298) can provide any assistance to the NDHM.

With warm regards
Yours sincerely,



Ranbir Singh

(A University of Law Established in 2008 by Act No. 1 of 2008 of Delhi)
Sector-14, Dwarka, New Delhi - 110 078 ☎ :+91 11 2803 4253 🖷:+91 11 2803 4256
✉ : ranbirsingh2107@gmail.com, vc@nludelhi.ac.in website: www.nludelhi.ac.in

CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY DELHI

COMMENTS TO THE NATIONAL HEALTH AUTHORITY ON THE DRAFT HEALTH DATA MANAGEMENT POLICY FOR NATIONAL DIGITAL HEALTH MISSION[°]

nludelhi.ac.in | ccgdelhi.org | ccg@nludelhi.ac.in

[°]Authored by *Arpitha Desai*, and reviewed and edited by *Sarvjeet Singh and Smitha Krishna Prasad*.

INTRODUCTION

Despite implementing lockdown measures and restricting the movement of people, the exponential increase in Covid-19 cases in India is evidence to show the vulnerabilities in India's existing public healthcare system. While higher fiscal dependence of states on the Centre, lack of budgetary resources, and weak forces of cooperative federalism may be reasons for poor healthcare facilities[1], the absence of a decentralized legal framework that protects the right to health has added to the challenges faced by the government and citizens during this health crisis.

Though the Indian Constitution does not contain any explicit provision for the right to health, the Directive Principles of State Policy in Part IV of the Indian Constitution[2] highlight the role of the Centre, states, and local governments in the provision of public healthcare through ensuring humane work conditions, providing maternity relief, raising nutrition levels, and improving public health. Furthermore, the Indian judiciary, in several cases[3], has read the right to the health within the fundamental right to life guaranteed under Article 21 of the Indian Constitution.

Towards this, it is commendable that the National Health Authority (the "**NHA**") under the Ministry of Health and Family Welfare (the "**MoHFW**") has proposed the National Digital Health Mission (the "**NDHM**"), the National Digital Health Blueprint, and Ayushman Bharat Pradhan Mantri Jan Arogya Yojna to create the necessary support network for a digital health infrastructure in India and ensure affordable healthcare for all. In light of the global pandemic, there has been an unprecedented need for a robust public healthcare infrastructure and universal health coverage.

As part of the NDHM, the Government has released the Draft Health Data Management Policy (the "**Draft Policy**") with the objective of creating a digital

[1] NITI Aayog, Ministry of Health and Family Welfare, Government of India, Healthy States Progressive India - 'Report on the Ranks of States and Union Territories' (2019) <http://social.niti.gov.in/uploads/sample/health_index_report.pdf>.

[2] Article 39 (E) directs the State to secure health of workers, Article 42 directs the State to just and humane conditions of work and maternity relief, Article 47 casts a duty on the State to raise the nutrition levels and standard of living of people and to improve public health. Moreover, the Constitution does not only oblige the State to enhance public health, it also endows the Panchayats and Municipalities to strengthen public health under Article 243G (read with 11th Schedule, Entry 23).

[3] *Bandhua Mukti Morcha v Union of India & Ors.* (1997) 10 SCC 549; *State of Punjab & Ors. v Ram Lubhaya Bagga* 1998 4 SCC 117.

ecosystem of personal health and medical records, which shall be voluntary and based on the informed consent of individuals participating in the ecosystem.

The Draft Policy governs the activities of all entities and individuals participating in the National Digital Health Ecosystem (the "**NDHE**"). It includes those who have been issued an ID under the Draft Policy, healthcare professionals, health care providers who collect, store and share health data in electronic form in connection with its transactions, drug manufacturers, medical device manufacturers, insurers, research bodies, and governing bodies such as the NHA and MoHFW.

While the Draft Policy may be useful in creating a National Health Stack as earlier contemplated by the NITI Aayog[4] to ensure continuum of care to patients, it is riddled with loopholes and ambiguities that may result in exclusions and data privacy violations.

A. PUBLIC CONSULTATION

Over the years, public consultation has become an essential tool in increasing transparency, enhancing public participation in law making, and ensuring efficiency of proposed regulations. Stakeholders have offered valuable insights and reforms for several policies across sectors, which has strengthened democratic processes. Since public health concerns the entire population, private service providers as well as the State, public consultation for the Draft Policy is key to enable smooth implementation of the NDHM.

At the outset, it is necessary to highlight that the Draft Policy was released on 26 August 2020 for public comments with an initial deadline of one week for feedback. This was challenged before the High Court of Delhi on the ground that it is inconsistent with the Pre-legislative Consultation Policy, 2014 that mandates a 30-day window for stakeholder comments[5] and excludes non-English speakers, persons with disabilities, and people without internet access. Based on the Delhi High Court's direction to the Central Government, while the MoHFW extended the deadline to 21

[4] NITI Aayog, Government of India, 'National Health Stack - Strategy and Approach' (2018) <https://niti.gov.in/writereaddata/files/document_publication/NHS-Strategy-and-Approach-Document-for-consultation.pdf>.

[5] Pre-legislative Consultation Policy, Legislative Department, Ministry of Law and Justice, Government of India, 5 February 2014 <http://legislative.gov.in/sites/default/files/plcp.pdf>.

September 2020 in compliance with the requirement, the concerns surrounding language and accessibility raise concerns about the process and manner in which public consultation for the Draft Policy is being undertaken. Especially when such a crucial piece of policy will impact millions of citizens amidst a pandemic, reasonable timelines and discourse is necessary.

Given that 'public health' is an entry in the state list of the Indian Constitution[6], any federal policy involving state participation as well as expenditure requires extensive consultation with state governments prior to public consultation. Furthermore, since stakeholders such as the civil society, health care professionals, health care providers, insurers etc. will play a key role in facilitating the implementation of the Draft Policy, they would require adequate time to organize and review the provisions of the Draft Policy to share substantive comments and feedback.

B. EXISTING LEGAL FRAMEWORKS

Though the Draft Policy forms part of the government's NDHM to ensure universal health coverage for all, several existing health information frameworks already address various concepts contained in the Draft Policy. This may result in overlapping of regulatory obligations under different frameworks and may cause confusion for individuals participating in the ecosystem. Therefore, in order to implement such a federated architecture at various levels, harmonising existing provisions should be undertaken by the different ministries which shall participate in this exercise.

Privacy Regulations

With the Draft Personal Data Protection Bill, 2019 (the "**PDP Bill**") pending before the Parliament and being examined by a parliamentary committee, India does not have a comprehensive data protection regime at present. While the Information Technology Act, 2000 (the "**IT Act**") read with the IT (Reasonable Security Practices, Procedures and Sensitive Personal Information) Rules, 2011 (the "**SPDI Rules**") govern the collection and processing of personal information and sensitive personal information, the applicable provisions have limited scope and are restricted to bodies

[6] Constitution of India 1950, Entry 6, List-II, Seventh Schedule.

corporate using individual data. Additionally, the SPDI Rules also do not have provisions that are specifically applicable to the State and may not be adequate to address potential harm caused or risks involved in the collection and processing of health data. Therefore, with no dedicated legal and regulatory framework for something as precarious as health data, the Draft Policy cannot be implemented in the absence of a data protection legislation.

Given that the right to privacy has been recognized as a fundamental right under the Indian Constitution in the case of *Justice K. S. Puttaswamy v. Union of India*[7] ("***Puttaswamy I***"), any intrusion to such right by the State in the interest of public health is only possible if proportionate to the lawful objectives of the State. While the said case recognizes public health as a valid ground on which restrictions may be placed on the right to privacy, it also imposes the duty of the State to maintain anonymity of individuals. While the Draft Policy is a well-intended policy, any law or policy intruding on sensitive personal data such as health data and medical records has to respect liberty, equality, and privacy of individuals. The Draft Policy appears to disregard the principles laid down in the *Puttaswamy I*, which states that any infringement of privacy by the State is permissible only if it passes the proportionality test laid down by the Supreme Court in *Puttaswamy I*, namely:

(i) The action must be sanctioned by law;

(ii) The proposed action must be necessary in a democratic society for a legitimate aim;

(iii) The extent of such interference must be proportionate to the need for such interference; and

(iv) There must be procedural guarantees against abuse of such interference.

While the above mentioned test is applicable to only State actors, there are no such safeguards applicable to non-State actors such as private insurance providers, medical device or fitness wearable manufacturers, health mobile applications etc. It is the responsibility of the State to bring in laws and regulation that ensure that adequate safeguards are available to protect citizens' rights.

[7] *Justice K. S. Puttaswamy (Retd.) and anr. v Union of India and ors. (2017) 10 SCC 1.*

Clinical Establishments and EHR Standards

The Clinical Establishments (Registration and Regulation) Act, 2010 (the "**CERRA**") regulates the registration of clinical establishments in certain states[8] and prescribes minimum standards of facilities and services, which such establishments provide. These include hospitals, maternity homes, nursing homes, dispensaries, clinics, etc. Among other conditions, the Clinical Establishment (Central Government) Rules, 2012 (the "**CE Rules**") require clinical establishments to maintain Electronic Medical Records ("**EMR**") or Electronic Health Records ("**EHR**").

In order to bring standardisation, homogeneity, interoperability in capture, storage, transmission, and use of healthcare information across various health IT systems, the MoHFW also notified the EHR Standards. While these standards have not been made mandatory, all states and union territories have been advised to adopt the EHR Standards in all the ICT applications in healthcare including in rural areas. However, the lack of IT infrastructure and constant supply of electricity in rural India, reluctance in adoption of EHR systems by practitioners, and incomplete coverage of Aadhaar have posed challenges in the implementation of EHR standards in India.

Digital Information Security in Healthcare Act

In 2018, the MoHFW floated the Digital Information Security in Healthcare Act ("the **DISHA**") with the objective of regulating the collection and processing of digital health data; ensuring privacy, confidentiality, standardization and security; and establishing the National Digital Health Authority and Health Information Exchanges. Though the MoHFW initiated its public consultation process and sought public comments on DISHA, there has been no communication from the Ministry regarding the status of the consultation or legislation.

[8] The Act has taken effect in the four states namely, Arunachal Pradesh, Himachal Pradesh, Mizoram, Sikkim, and all Union Territories except the NCT of Delhi since 1 March, 2012 vide Gazette notification dated 28 February 2012. The states of Uttar Pradesh, Uttarakhand, Rajasthan, Bihar, Jharkhand, Assam and Haryana have adopted the Act under clause (1) of article 252 of the Constitution.

Other Regulations

In addition to the above discussed frameworks, sector-specific regulations that govern the sale of drugs and medical devices[9], pharmacies[10], insurance providers[11], tele-medicine providers[12], etc. also require a thorough analysis so as to align the provisions and requirements.

C. Lack of Adequate Technical, Institutional, and Legal Knowledge and Public Health Infrastructure

In 2005, the United Kingdom's National Health Service attempted to digitize health records of its entire population by 2010 in order to increase efficiency and reduce medical errors in the healthcare system. However, despite high volumes of investment in the project, it failed to achieve its main objectives of establishing an integrated electronic health record system[13]. Due to unrealistic timelines, failure to address issues of patient confidentiality, and interoperability, the project was dismantled after an estimated cost to the UK taxpayer was over £9.8 billion, which is considered to be one of the expensive healthcare IT failures[14].

In the past few years, the Indian government has also made several attempts to digitize health records and build a federated architecture for participants in the healthcare ecosystem. This includes the NITI Aayog's proposed National Health Stack, the MoHFW's National Digital Health Blueprint, the MoHFW's Health Management Information System, and the Digital Information Security in Healthcare Bill, 2018. However, such initiatives have not been entirely successful owing to factors such as lack of institutional capacity, technical know-how, and inordinate delays. Since such a framework would require efforts from several government ministries and departments such as *inter alia* the MoHFW, Ministry of Electronics and Information Technology (the "**MeitY**"), Ministry of Women and Child

[9] The Drugs and Cosmetics Act 1940.
[10] The Pharmacy Act 1948.
[11] Insurance Regulatory and Development Authority of India (Health Insurance Regulations) 2016.
[12] Telemedicine Practice Guidelines 2020.
[13] Diptasri Basu, 'The Electronic Health Records System in the UK' (*Centre for Public Impact*, 3 April 2017) <https://www.centreforpublicimpact.org/case-study/electronic-health-records-system-uk/>.
[14] 'NHS IT system one of 'worst fiascos ever' says MPs' (*BBC News*, 18 September 2013) <https://www.bbc.com/news/uk-politics-24130684>.

Development, local government bodies, etc., adequate training for all those making data entries is required for accuracy and efficiency.

From a privacy perspective, creating and maintaining such a large network of data systems and servers will require all participants to adopt security procedures and standards to mitigate emerging threats and vulnerabilities. Since the security of sensitive personal data including health data is crucial to prevent any harm caused to patients, ensuring that the digital ecosystem comprises secure hardware and software is of utmost importance. Cyber attacks on hospitals and clinics have far graver implications than attacks on organizations operating in other industries. Any illegal access to personally identifiable information of patients such as addiction histories, suicide attempts, crimes against women, etc. may put the patient at severe risk.

The Draft Policy mandates the adoption of international standards, however, enforcement of such requirements is not feasible. In the event that there is any attack to the IT infrastructure of healthcare providers, patient health may be at high risk owing to delays in providing medical care and may result in significant harm.

The response to and management of Covid-19 has highlighted the need for coordination between the Centre and states. It has also demonstrated the lack of capacity building at district and local levels where prevention of the pandemic required greater attention. Therefore, it is imperative to decentralize the power and funds so as to strengthen state-level and local healthcare systems.

D. CONSENT

Legal Framework for Informed and Specific Consent

In the context of healthcare, confidentiality and privacy of the patient is of utmost importance and any digital health system involving both the public and private sectors must factor in and respect the autonomy of the patient. The first layer of building such a digital health system is informed consent and data ownership of the individuals participating in the system.

The concept of informed consent has been debated in several cases, with its scope being described by the courts to mean the grant of permission by a patient for an act to be carried out by a doctor, such as a diagnostic, surgical or therapeutic procedure[15]. The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 as laid down by the Medical Council of India (the "**MCI**") also requires physicians, before performing an operation, to obtain in writing, the consent from the husband or wife, parent or guardian in the case of minor, or the patient himself as the case may be, failing which such physician may be held liable for professional misconduct. Similarly, the Drugs and Clinical Trial Rules, 2019 issued under the Drugs and Cosmetics Act, 1940 mandate obtaining prior written consent of the study subjects participating in new drugs or clinical trials[16]. Though the SPDI Rules notified under the IT Act require bodies corporates to obtain prior written consent from individuals for the collection and processing[17] of sensitive personal data[18], the Draft Policy expands the scope of sensitive personal data, which does not enjoy adequate protection under the SPDI Rules.

At present, there is no such legal framework which governs user consent for the collection and processing of sensitive personal data or such that confers the right of ownership over data on the individual. While the Draft Policy borrows the threshold for informed consent for the collection and processing of personal data including sensitive personal data from the PDP Bill, the PDP Bill is yet to receive parliamentary assent. Therefore, to ensure the data privacy of individuals, any policy such as the Draft Policy should be implemented only after enacting a strong data protection law with an independent regulator. The lack of a legal consent framework also means that the requirement of consent will be of the private entity or government body collecting and processing personal data, which is arbitrary and illegal.

---

[15] *Samira Kohli v Dr. Prabha Manchanda and Another* (2008) 2 SCC 1.

[16] Drugs and Clinical Trial Rules, 2019, Third Schedule.

[17] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rules 5, 6, and 7.

[18] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3 defines 'sensitive personal information' to mean such personal information which consists of information relating to - (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; and (vi) biometric information.

Having said the above, the consent framework in the context of healthcare should be revised basis the following factors:

(i) **Digital Penetration**: Given that the Draft Policy envisages creating repositories of health data at different levels, it should factor in the technical capacity of healthcare institutions across the country. Since access to computers, smartphones, and the Internet remains scant in rural India, building a digital architecture with poor infrastructure may be counterproductive.

(ii) **Literacy Rates**: It is a well-known fact that levels of adult literacy in India vary across states and are relatively poorer in rural India than urban India. Since digital literacy would entail additional knowledge of understanding the digital product or service, any consent framework including notice requirements should take into consideration the various levels of literacy and digital literacy to ensure that consent provided by the individual is informed and specific.

(iii) **Consent Fatigue**: As the Committee of Experts set up by the MeitY under the Chairmanship of Justice B.N. Srikrishna (the "**Justice Srikrishna Committee Report**") had indicated, there exist many boilerplate agreements in the digital world and people consenting to such agreements often do not read or understand the terms and conditions at the time of providing consent. Owing to the many boilerplate agreements people sign up for on a daily basis, the consent fatigue caused may result in uninformed consent, which undermines the autonomy of the individual.

Storage of Data

The Draft Policy does not contain any specific provisions dealing with the storage of health data by data fiduciaries. Since both public and private data fiduciaries will need to store highly sensitive data on their servers, the physical and digital security of such infrastructure must be periodically reviewed to prevent any unauthorized use of data. The Draft Policy should contain sufficient safeguards for the encryption of health data stored on the data fiduciaries' servers.

For example, in the United States, the Health Insurance Portability and Accountability Act (the "**HIPAA**") sets out physical and digital safeguards[19] to protect sensitive health information. Healthcare organizations are required to comply with technical requirements and hosting standards so as to ensure the security of their data centers. Additionally, for physical safeguards, HIPPA requires organizations to implement adequate measures to restrict access to data.

Revocation of Consent and Deletion of Personal Data

Though the Draft Policy is voluntary in nature and participants have the option to revoke previously given consent, permanent erasure of such data is not possible. Clause 14 (ii) of the Draft Policy sets out the rights of the data principal and the specific circumstances in which the data principal may request for erasure of their data. This includes if the storage of personal data is in violation of data protection principles or if the purpose for which it had been initially collected has been satisfied. However, the determination of whether personal data of individuals should be retained is to be done by the data fiduciary, which in turn, does not allow the data principal to exercise control of his/her data. Though the Draft Policy confers upon the data principal the right to delete his/her data from the digital locker, it is silent as to whether such deletion is permanent. Therefore, the Draft Policy should adopt an approach that favours the rights of the data principal and holds the data fiduciary or processor more accountable with respect to the personal data it collects and processes.

Child Consent/ Mentally/ Differently Abled

When it comes to healthcare, consent obtained from children and physically/mentally ill patients is of utmost importance as such consent would need to meet a different threshold of consent in comparison to traditional consent provided for the collection and processing of personal data. Given that such persons may not have adequate physical or mental capacity to provide informed and specific consent, any decisions based on prior consent provided by such person or persons authorized by them should solely be in their interests. Similarly, any fresh purpose for which their data

[19] HIPAA Security Rule, 45 CFR Part 160 and Subparts A and C of Part 164.

may be used without their consent must also be for their physical and mental well-being.

While the Draft Policy contemplates a consent framework whereby the parent/legal guardian would provide consent on behalf of a child or whereby a nominee (authorized by the person) will provide consent on behalf of the seriously or mentally ill person, it does not account for situations of medical emergencies, where patients require immediate care.

Further, the Draft Policy neither defines 'medical emergency' nor does it provide adequate guidance on processing personal data during medical emergencies, where obtaining informed consent may not be possible.

Section 12 of the PDP Bill allows for the processing of personal data without consent of the data principal to respond to any medical emergency involving a threat to the life or a severe threat to the health of any individual and to provide medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health. However, the PDP Bill also fails to define the scope of a medical emergency. Without delineating the concrete contours of a medical emergency, collection and processing of personal data may be misused and even illegal. Any policy, which is specific to health information privacy, ought to factor in exceptional circumstances and provide adequate protection to patients who are incapacitated and cannot provide informed and specific consent.

E. SCOPE OF HEALTH DATA

Similar to the PDP Bill, the Draft Policy defines sensitive personal data to mean "*such personal data, which may reveal or be related to, but shall not be limited to… financial information such as bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health data; sex life; sexual orientation; medical records and history; biometric data; genetic data; transgender status; intersex status; caste or tribe; and religious or political belief or affiliation*". Additionally, health data under the Draft Policy also includes within its ambit electronic health records, electronic medical records, personal health records, and personal health identifiers.

However, the Draft Policy makes no reference to the PDP Bill or the definitions borrowed therefrom and in fact, introduces new definitions, which do not enjoy the force of law. Not only may this result in confusion once the PDP Bill is enacted, it also poses severe challenges in terms of over collection of sensitive personal data and subsequent remedies to be sought without any legislative backing. Furthermore, requiring individuals to provide information such as transgender status, religious or political belief or affiliation may in turn, leaves scope for discrimination on the basis of such information.

F. LINKAGE TO AADHAAR AND PRIVATE ACCESS TO PERSONAL DATA

The Draft Policy envisages the creation of a health ID (for individuals, practitioners, as well as establishments), which will act as a repository of personal data including health data of individuals participating in the digital ecosystem as well as the data possessed by healthcare providers such as hospitals, diagnostic laboratories, insurance companies, online pharmacies, telemedicine firms, etc. In order to generate this ID, individuals and healthcare providers are required to furnish their Aadhaar IDs, which will, in turn, be used by a range of other public and private sector healthcare providers. The Draft Policy is silent as to why there is a need for another separate ID, when Aadhaar already exists. Though the Draft Policy does not mandate the use of Aadhaar for authentication, it leaves the discretion of deciding other means of authentication to the NHA. Despite the Supreme Court's ruling and past experiences, Aadhaar related exclusion[20] has proven that from being a voluntary ID, it has become de facto compulsory for most welfare programmes[21].

Further, this digital ID raises concerns with respect to violating the judgment in the case of *Justice K. S. Puttaswamy v. Union of India*[22] ("***Puttaswamy II***"), which read down the provisions contained in the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (the "**Aadhaar Act**") that allowed

[20] Karthik Murlidharan et al, 'Identity Verification standards in welfare programs: experimental evidence from India' (*NBER*, 2020) <https://faculty.virginia.edu/sandip/MNS%20JH%20ABBA.pdf>; Dalberg, 'State of Aadhaar: A People's Perspective' (2019) <https://stateofaadhaar.in/assets/download/SoA_2019_Report_web.pdf>.

[21] Reetika Khera, 'Impact of Aadhaar on Welfare Programmes' (*The Economic and Political Weekly*, 16 December 2017) <https://www.epw.in/journal/2017/50/special-articles/impact-aadhaar-welfare-programmes.html>.

[22] *Justice K. S. Puttaswamy (Retd.) and Anr. v Union of India and Ors.* (2019) 1 SCC 1.

for sharing of sensitive personal data by the government with private companies[23] and highlighted the risks involved. In Puttaswamy II, the Supreme Court specifically prohibited the use of Aadhaar by private entities on the grounds that it would result in commercial exploitation of data and thereby, impinge on the individual's right to privacy. Therefore, under Section 7 of the Aadhaar Act, only such subsidies, benefits or services that draw expenditure from the Consolidated Fund of India would require Aadhaar authentication. However, by way of the Aadhaar and Other Laws (Amendment) Act, 2019, private entities are now permitted to carry out Aadhaar-based authentication, provided such authentication is allowed for under the provisions of any other law passed by the Parliament[24].

Reading the principles laid down by the Supreme Court with the Draft Policy, the use of Aadhaar for facilitating the digital health ecosystem is not backed by the law. The Draft Policy, which also involves the participation of both public and private parties to access Aadhaar data would also dilute the scope of Section 7 of the Aadhaar Act. Since the objective of private businesses would involve capitalization of health data, allowing such entities to participate with a publicly linked ID would have serious repercussions with inadequate procedural safeguards in case of any harm caused.

Similar to Aadhaar-based welfare disbursement, the Estonian government has established an ID card based digital infrastructure under the Population Register Act, 2019 (the "**PRA**") and the Identity Documents Act, 2000 (the "**IDA**"), which offers its citizens various welfare programmes. The National Health Information System allows both public and private healthcare providers to connect to the health information system and store EHRs centrally. Though the IDA allows for private entities to provide e-services, it permits public service providers to restrict such provision to ensure safe use thereof[25]. Additionally, Section 44 of the PRA permits government agencies to access data for the "performance of public duties" as well as natural and

[23] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, s 57.
[24] Aadhar and Other Laws (Amendment) Act, 2019, s 6 (amendment to s 4 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
[25] Identity Documents Act 2000, s 20.

legal persons "with a legitimate interest"[26]. While the objectives of the law have been specified for both public and private actors, there is no such demarcation in the Draft Policy.

G. SURVEILLANCE

With countries grappling with Covid-19, governments worldwide have deployed various technology based tools for contact tracing and enforcing lockdown or quarantine measures. Even the World Health Organization has issued a guidance document to member states for the implementation of 'public health surveillance' for Covid-19[27]. In India, the Centre and state governments have also used such public health surveillance measures, however, with no legal basis. For example, 'Aarogya Setu', a mobile application which was launched by the government to facilitate contact tracing among infected persons using Bluetooth and GPS, was severely criticized for subverting civil liberties through overcollection of personal data (such as gender, caste, etc.) and lack of adequate safeguards within the code[28]. Due to the trust deficit that was created by mandating Aarogya Setu without any legal basis, the government eventually made downloading the application voluntary[29] and published the source code of the application[30].

Pursuant to this, the MeitY published the Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020[31] (the "**Protocol**"), which makes the MeitY and National Informatics Centre responsible for the collection, processing, and managing response data collected by the Aarogya Setu application and sets out the data

[26] Population Register Act, 2019, s 46 and 51. Legitimate interest has been defined as "the protection of the life, health, rights and freedoms of the applicant or another person," "performance of a contract entered into with the applicant or for ensuring performance of the contract."

[27] World Health Organization, 'Public health surveillance for Covid-19: interim guidance' (7 August 2020) <https://www.who.int/publications/i/item/who-2019-nCoV-surveillanceguidance-2020.7>.

[28] Smitha Krishna Prasad and Kritika Bhardwaj, 'Surveillance Without Safeguards in the Pandemic' (*Article 14*, 30 April 2020) <article-14.com/post/pandemic-in-india-spurs-surveillance-without-safeguards>.

[29] Aashish Aryan, 'Centre signals shift in stance: Aarogya Setu app no more mandatory' (*The Indian Express*, 18 May 2020) <https://indianexpress.com/article/india/centre-signals-shift-in-stance-aarogya-setu-app-no-more-mandatory-6414878/>.

[30] Press Information Bureau of India, 'Aarogya Setu is now open-source', 26 May 2020 <https://pib.gov.in/PressReleasePage.aspx?PRID=1626979>.

[31] Ministry of Electronics and Information Technology, Government of India, 'Aarogya Setu Data and Knowledge Protocol, 2020', 11 May 2020 <https://www.meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf>.

protection principles that shall be followed for this purpose. The Protocol permits sharing of response data with Government ministries, departments, public health institutions, and local governing bodies to formulate and implement appropriate health responses, which shall be used by such entities in a fair, transparent, and non-discriminatory manner. However, there is no clear definition of 'appropriate health responses', which goes against the principle of proportionality and purpose limitation and may impinge on the right to privacy.

In wake of the pandemic, the government has invoked the Epidemics Diseases Act, 1897 and Disaster Management Act, 2005 for its management. However, both legislations fail to provide adequate legal basis for deploying surveillance tools to curb the spread of the virus. While governments enjoy residuary powers under these laws to take necessary steps to prevent the transmission of any disease in the interest of public health, there is no system of checks and balances or legal oversight to prevent any abuse caused by such surveillance. The use of such technology is disproportionate and invasive, which is contrary to the threshold laid down by the Supreme Court in *Puttaswamy I*. Not only do such technological solutions threaten individual privacy, it also risks becoming the "default option" for addressing public crises[32]. Therefore, to prevent any such intrusive measures by the State, it is imperative for the legislature to enact a data protection framework which will provide adequate legal sanction to any surveillance tools, account for public emergencies and health crises, and have sufficient judicial oversight to safeguard fundamental rights.

While the legal basis for State-sponsored surveillance can be challenged before courts, the growth of 'Big Tech' is paving the way for surveillance capitalism[33], which relies on the commodification of personal data through online surveillance. In the context of healthcare and especially during public health emergencies, tech corporations have capitalized on user data through innovations such as facial recognition technology, drones, fitness trackers, etc. With Big Tech companies are

[32] Evgeny Morozov, 'The tech 'solutions' for coronavirus take the surveillance state to the next level' (*The Guardian*, 15 April 2020) <https://www.theguardian.com/commentisfree/2020/apr/15/tech-coronavirus-surveilance-state-digital-disrupt>.

[33] Shoshana Zuboff, 'A Digital Declaration: Big Data as Surveillance Capitalism' (*FAZ.NET*, 15 September 2014) <https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshan-zuboff-on-big-data-as-surveillance-capitalism-13152525.html>.

now assisting governments in managing the pandemic[34], risks of corporate interests being furthered through political sanction raises concerns surrounding privacy and ethics.

G. ANONYMIZATION OF PERSONAL DATA

Having regard to the sensitivity of health data, clause 29 of the Draft Policy contemplates various purposes for which data fiduciaries would be required to carry out anonymisation or de-identification of data prior to sharing such data with other data fiduciaries or processors. It also requires the NHA to set out the procedure for accessing such anonymised or de-identified data and periodically review the technical processes and protocols for the same.

Under the PDP Bill, anonymisation has been defined as the "*irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Authority*"[35]. Since the PDP Bill is yet to receive legal sanction, the Data Protection Authority (the "**DPA**"), though empowered to issue codes of practise for the methods of de-identification and anonymisation of personal data, has not yet notified any such standards. However, the Draft Policy sets the standard for anonymisation as "*any means reasonably likely to be used to identify such data principal*". Since health data is of critical nature and is susceptible to misuse if re-identified, the DPA and NHA should ensure harmonization of standards for anonymisation and de-identification under both frameworks.

There is vast evidence to show that irreversible anonymisation of data is rarely possible and there always exists a risk of re-identification of data[36]. Such re-identification is possible by combining different data sets or using new techniques, which may pose adverse risks and cause irreversible harm to those who have been

[34] Leo Kelion, 'Coronavirus: First Apple/Google-based contact tracing app launched' (*BBC*, 26 May 2020) <https://www.bbc.com/news/technology-52807635>.
[35] Personal Data Protection Bill, 2019, s 3(2).
[36] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 'A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians' (2019) <https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf>; Ministry of Electronics and Information Technology, 'Report by the Committee of Experts on Non-Personal Data Governance Framework' (2020) <https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf>.

re-identified. While Section 82(1)(a) of the PDP Bill provides for offences and penalties with respect to re-identification of de-identified personal data, it does not punish re-identification of anonymised data. In this regard, the Draft Policy provides limited safeguards and no remedies for data principals whose data may be compromised because of re-identification. Therefore, it is recommended that to ensure patient confidentiality and privacy, adequate mitigation strategies to prevent re-identification of anonymized and de-identified personal data must be incorporated into the PDP Bill and Draft Policy.

H. DATA BREACH AND NON - COMPLIANCE

With the world moving online in light of the global health crisis, dependence on digital services has increased multifold. Since the outbreak of Covid-19, organisations have reported a significant spike in data breaches[37]. Not only have hackers obtained unauthorized access to Covid-19 patient data[38], several government authorities have also failed to implement adequate cybersecurity measures to protect personal data of infected patients[39]. In response to such incidents, even the Kerala High Court injuncted Sprinklr, a New York based data analytics company from misusing Covid-19 data entrusted to it by the Kerala state Government and directed it to obtain informed consent from citizens prior to collection and anonymise such data[40].

Given that the Draft Policy aims to establish a decentralized digital health system with public and private entities having access to sensitive personal data, security and data privacy of such systems is quintessential to ensure patient confidentiality. Additionally, hospitals and diagnostic laboratories are now relying on EMRs given that the CE Rules issued under the CERRA mandate the "maintenance and

[37] Prashasti Awasthi, '66 per cent Indian firms reported data breaches during remote working: Survey' (*The Hindu Businessline*, 21 August 2020) <https://www.thehindubusinessline.com/info-tech/66-per-cent-indian-firms-reported-data-breaches-during-remote-working-survey/article32410661.ece>.

[38] Joe Wallen, 'Hackers obtain Covid-19 patient database in protest at treatment of Indian health workers' (*The Telegraph*, 1 July 2020) <https://www.telegraph.co.uk/global-health/terror-and-security/hackers-obtain-covid-19-patient-database-protest-treatment-indian/>.

[39] Suraksha P., 'Privacy of suspected COVID-19 patients breached' (*Deccan Herald*, March 6, 2020) <https://www.deccanherald.com/national/privacy-of-suspected-covid-19-patients-breached-810992.html>.

[40] W.P.(C).Temp No. 84, 129, 132, 148 and 163 of 2020.

provision of EMR or EHR for every patient" for the registration and continuation of every clinical establishment[41].

While the Draft Policy requires data fiduciaries to formulate and implement a personal data breach management mechanism, it fails to provide adequate remedies to aggrieved individuals in case of a data / security breach (for example, compensation) and does not require data fiduciaries to mandatorily report such breaches to the data principals or even the public. However, it requires data fiduciaries to report breaches to the NHA, which may further notify the Indian Computer Emergency Response Team (the "**CERT-In**") as may be required under applicable laws. The regulatory powers of the CERT-In, which is the nodal agency on responding to cybersecurity incidents in India, has often been questioned for its interaction with sector-specific regulators such as the Reserve Bank of India or Securities and Exchange Board of India[42]. Given that the PDP Bill will establish the DPA, which in turn, will interact and consult other regulators, any provisions related to data breach management should be in consonance with the proposed data protection framework.

Unlike other jurisdictions, at present, there is no law mandating clinical establishments to disclose data or security breaches. For example, in the United States, the HIPAA, which is the primary law for health information privacy, requires a hospital to disclose a breach which has affected more than 500 patients[43]. However, the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013, which prescribes mandatory breach notification requirements for private entities, does not provide any such statutory obligation for State actors. Given that a majority of the population relies on public health care, any data breach resulting in harm to the individual may go unscrutinized.

[41] Clinical Establishment (Central Government) Rules, 2012, Rule 9(iv).
[42] Udbhav Tiwari, 'Cyber Security & the CERT-In A Report on the Indian Computer Emergency Response Team's Proactive Mandate in the Indian Cyber Security Ecosystem' (*Centre for Internet & Society*, 19 November 2016) <https://cis-india.org/internet-governance/files/cert-ins-proactive-mandate.pdf>.
[43] HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414.

Though the Draft Policy does not prescribe descriptive offences and penalties, any violation of or non-compliance with the Draft Policy may result in (i) the cancellation or suspension of the ID issued under the Draft Policy; or (ii) the termination of services/contracts. In addition to (i) and (ii), the Draft Policy also specifies that any action under any applicable laws may also be initiated. However, it is unclear how such applicable laws will interact with the Draft Policy given that many such laws may have contradictory provisions.