Journal of Law and Legal Research Development

Digital Health Services Through the Lens of Data Privacy

Indumathi S

Assistant Professor, School of Law, SASTRA Deemed to be University, Thanjavur

Article History

Received: Apr-2024
Revised: Apr-2024
Accepted: Apr-2024
Published: Apr-2024

Keywords

Unique Digital Health ID
Health Data Privacy
Informed Consent in Digital Health
Digi Locker
Data Management Policy

Abstract

Pandemic has showcased to the world the need for having seamless health data exchange. One of the major reasons for India's success in vaccinating her vast population is use of digital technology to ensure an easy mechanism for the people to register for vaccinations, get appointment dates as well as the jabs itself. This ease of use has made even the rural population appreciate the need for seamless data exchange to provide excellent health care. Keep this viewpoint in mind, the Indian government has chosen to usher in unique health id for each person based on their KYC / Aadhar card number. This is a welcome change albeit riddled with privacy concerns. In this article the author seeks to analyze the strength of digital health data framework upon the touchstone of privacy and informed consent. The author seeks to find out if the existing policies and laws are strong enough to ally privacy concerns or if there is an emergent need to ensure that unique digital health id does not result in data and privacy breaches across the digital health data framework. The author also seeks to find out if the data policies of the government are followed in practice at the ground level, wherein the people might be unaware of 'informed consent.'

Corresponding Author:

Indumathi S

Assistant Professor, School of Law, SASTRA Deemed to be University, Thanjavur

1. INTRODUCTION

E-Governance refers to usage of ICT at various levels of government and publicsector to enhance governance. Sustainable Development Goals guides the governmentsto ensure equitable access of health care services to all men and women. The need for universal equitable access to health care was very much felt during the recent Corona Virus Pandemic. In a country as vast and as populous as India successful vaccination was possible only because we had a mechanism to deliver e-health services. The pandemic has also showcased that the reach of e-governance / e-health services to the rural population even in the most interior inaccessible parts of India is not impossible. E-Health services provided by Arogya Setu as well as Co-Win app provided a mechanism through which any person can get appointment to receive vaccination as well as get a digital certificate of vaccination after the vaccinations are completed. Aroyga Setu app also provided a mechanism through which the common man was alerted when he came into close proximity with any corona virus affected person. These e-health services app for the very first time gave common man a taste ofefficient functioning of the government health services. It prominently showcased ease of doing business, in sense that the common man was no longer required to needlesslystand in long queues for days together to receive vaccination services. These apps are able to recognize the people on basis of their unique Aadhar Card ID which they must provide to authenticate themselves, thereby streamlining the services as well as ensuring non-duplication of requests. After vaccination process was completed, the digital certificate for the same can be obtained from Digi Locker, which is also linked to our unique Aadhar ID card. The certificates were made easily available across all platforms including mobile phones, which yet again ensured ease of business when people wanted to travel from one state to another within India or travel even outside India. This ease of receiving health services are now knowing to all common men in India,therefore they will not be averse to storing electronic records of health-related data. Therefore, now the government has slowly started to pitch in for Unique Digital Health Identity (UDHI).

Availability of Unique Digital Health Identity over a period of time that there will be seamless transfer of Data from one health service provider to another. It might also provide various other benefits such as:

- Availability of the entire patient history at perhaps a finger stroke of thedoctor, if needed.
- An intervention can be setup to ensure that a prescription is not filled more than once, which will in turn help us in reduce drug abuse by patients.
- Provide easy mechanism to approach for second opinion or expert opinion, as all relevant data including lab results can be made availableeasily in electronic format.
- In cases of emergency health crisis of the patient, relevant data can be made available at once at a single keystroke instead of relying upon relative's / care takers to provide relevant medical history or medical files in physical form.

It is equally important to understand that in spite of all these benefits there are also certain concerns relating to privacy that needs to be answered. It cannot be a case of over enthusiasm rather we need to approach digital health services with abundant note of caution as it throws open confidential information of an individual to various public as well as private sector entities. In essence it might open doors to cyber security threats including breach of data as well as spamming spoofing and other allied nefarious activities, leading to severe lash backs from which we cannot easily recuperate. In this paper the author seeks to study the draft policies with respect to digital health through the lens of privacy laws and policies standards applicable globally and explore how well the policies are drafted and if any changes are required to meetinternational standards.

2. UNIQUE DIGITAL HEALTH IDENTITY (UDHI)

Primarily the genesis of UDHI can be traced back to National Health Policy 2017 as well as Niti Ayaog's National Health Stack 2018, based on which the National Digital Health Blueprint [NDHB] was drafted in 2019. This NDBH gives us a basic idea of the entire digital health infrastructure is to be formulated maintained and executed. It also gives an idea about the privacy concerns that is the primary focus of this research paper.

The key objectives of NDHB stipulates the following:

- Establishing and managing core digital health database with a seamless mechanismfor exchange of data.
- Creation of personal health records based on international standards while ensuringeasy accessibility of data to both the patients [who are referred as data principals] as well as various service providers.
- Methodology through which we can promote health data analytics and medical research establishing data ownership pathways to ensure that data is anonymized for research purposes or data is used on basis of patients' consent alone. In fact, even data collection requires data principal's consent. While giving consent itself the principal must be made aware of the purposes for which the data is collected.

The Blueprint mainly aims to 'capture data once and use it many time and ensure that we move away from 'data silos to systems.[1]' When we glimpse both at our National Health Policy 2017 as well as the Blueprint it at once becomes clear that the inspiration for the same was actually derived from ***Sustainable Development Goals*** [SDGs]. The SDGs consists are nearly 17 goals that are closely interconnected with oneanother and focuses of enabling all world nations to achieve the Millennium Development Goals. It includes health related goals also such as promoting good life expectancy. Providing immunization, eradicating malnutrition, ensuring disease control through equitable access to health services. To ensure all these and much morethe National Health Policy as well as Blueprint calls for Unique Health Identifier.

The Blueprint addresses concerns towards data privacy and confidentiality by ensuringthat:

- Duplication of efforts are reduced by establishment of National Health Stack whichwill also serve the purpose of convergence of IT infrastructure wherein privacy policies are addressed ab-initio.
- The entire data architecture is to be at three levels, to ensure there is decentralizationof data collection as well as storage and maintenance, namely shown in figure 1.
    - National Level
    - State Level
    - Facility Level

[1] *Ministry of Health and Family Welfare, Government of India (2019.) National Digital Health Blueprint, Retrieved from: https://main.mohfw.gov.in/sites/default/files/Final%20NDHB%20report_0.pdf.*

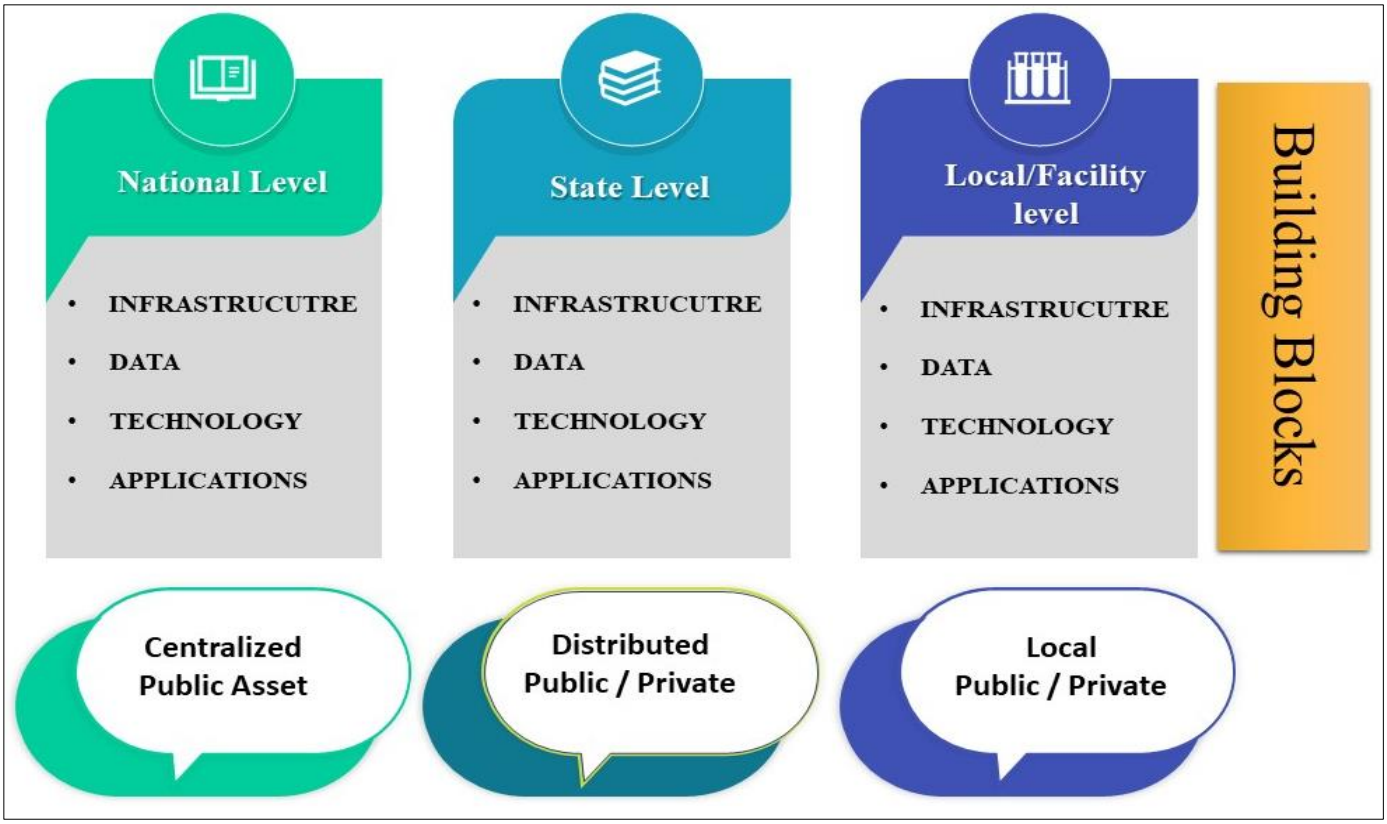

Fig 1: Entire data architecture of decentralizationof data collection

Federated Architecture of NDHB[2]

- The data is to be held at *Point of Care / closest possible physical location.*
- The citizens at all point in time must be empowered to have full control of theirpersonal health data as well as it's processing.
- Any service provider or software application can access these data only with theconsent of the data principal.
- The data so collected / processed can be stored with *Data Fiduciaries* includinggovernment agencies or other private large data storage facilities.
- Any other health facility service provider can avail the services of these licensed fiduciaries who act as data repositories, with the consent of the data principal.

This streamlined mechanism will pave way for both enabling data privacy as well as fixing liabilities upon the data fiduciaries in cases of any breach of laws. The fiduciaries as well as any entities who process the data will be responsible for both validity of the data as well as data protection obligations and compliances under applicable laws.

3. BUILDING BLOCKS

To ensure creation of unique ID as well as to ensure privacy security and confidentialityof data, the Blueprint envisages a series of building blocks based on which the entire digital health infrastructure is to be built. There are 23 such building blocks including:

- A building block for creating unique health ID and Health Locker through which data can be electronically created, stored, retrieved and amended / appended.
- A building block for consent management as well as a building block to anonymize data and take care of data privacy as *'a-priori'* instead of being retrofitted as an afterthought[3].
- Building blocks to enable establishing dedicated e-portals for health services as well as providing applications (mobile apps) for easy accessibility through mobile phones.
- Building blocks to ensure seamless interoperability between all the various components of the infrastructure.

3.1 Anonymizer

This seeks to ensure that all personal data are removed and full de-identification of therecords are achieved. The anonymizer will require to remove information that can identify thedata principal such as[4]:

[2] *Ibid, Pg 14.*
[3] *Ibid, Pg 6.*

[4] *Ministry of Health and Family Welfare Government of India (2016), Electronic Health Record (EHR) Standards-2016, retrieved from https://www.nhp.gov.in/.*

- Name
- Address
- Mobile numbers
- Email address
- Bank account number / insurance policy numbers
- Unique health identity assigned to the data principal
- Any vehicle numbers
- AADHAR card, PAN card, Passport and similar such ID numbers
- Fingerprints and other biometrics
- Any photographs if available etc.

Thus the anonymizer must be capable of removing all such information and de- identifying data in situations wherein the same is not required, such as let say research or analysis purpose. The anonymizer therefore will have the two pronged job of ensuring data authenticity and ensure that data cannot be traced back to the data principal. The data can be provided in this manner to even government agencies and authorities who seek to access healthrecords to handle critical monitoring of spread of notified diseases and so on.

3.2 Interoperability

Interoperability is to be made seamless in order to ensure smooth functioning of the entirehealth data infrastructure for the following purposes:

- Identification of administrators, patient demographics, care provider details as well asphysicians' details, being easily available to all who have the data principal's consent.
- Easy mechanism to retrieve history of the patient his previous diagnosis and even hisfamily member's health history if required.
- Collation of all vital data such as birth death, pregnancy as well as other wellnessindicators.
- Identification of adverse events or markers such as allergies, allergens and intolerance.
- Listing out all the medications, lists of all immunizations received the type of life stylefollowed as well as diet to be enforced.
- All information related to administration such as request for appointments, date ofadmission as in-patient, date of discharge transfer to another service facility etc.
- All aspects related to finances, bank accounts and insurance coverage details if any. As seen, the above list makes it pretty obvious that the creation of data, it's access and modification involves multiple players there is a very immediate concern of data validation.To ensure the same the following parameters have been set[5]:
- Records cannot be modified or deleted without following due process, as laid downby laws, rules, regulations or guidelines.
- Whenever any amendment or change is made the earlier version of the data must also be stored separately. The earlier versions are to be marked as inactive while the latest amended version will be marked as active record and available for easy retrieval.
- An audit log book must be diligently maintained to record every creation, access, modification or deletion of data so that the source of such transaction can be easily traced to check for reliability based on e-signature.
- Above all the infrastructure must also ensure that the data principal can log in and access his own health records as well as make decisions on whom he authorises toview or modify his records and for what purpose the access is granted.

3.3 Consent Manager

This is the most important building block which must seek to ensure that MeitY (Ministry of Electronics and Information Technology) rules for obtaining consent from the patient's / data principal is explicitly followed every time there is a need to access health records.This building block must ensure the patient is the data principal and that he is in full control of who can collect his data, store it, at what points in time it can be collected for what purposes itcan be shared and with whom the health record can be shared. The Blueprint very clearly states that the Consent Manager building Block must adhereto the standards set by both the IT Act 2000 as well as the Data Protection Bill that will be enacted in the future.

3.4 Health Locker

This building block can be equated with that of Digi Locker. The availability of Digi locker is coupled with that of AADHAR card number, in a similar manner availability of HealthLocker is tied up with unique health identifier. Data links are stored in the Health Locker whichcan be accessed by clinics / hospitals on a need-to-know basis. Essentially it means that their credentials are validated and an automatic check is run to ensure if they have obtained the consent of the data principal to view / modify his health record.
The presence of a Health Locker is supposed to provide ease of availing health servicesno matter in which remote part of India the Data Principal is currently situated. The Blueprintalso mandates that the Data Principal in spite of owning a Health Locker can choose to removehis digital footprint by exercising his 'right to be forgotten' choice, when

- The purpose for which the data was collected has been fulfilled or served, or
- Consent of the Data Principal has been withdrawn.

[5] *Ministry of Health and Family Welfare, Government of India (2019.) National Digital health Blueprint, Pg. 36,Retrieved from: https://main.mohfw.gov.in/sites/default/files/Final%20NDHB%20report_0.pdf*

4. HEALTH DATA MANAGEMENT POLICY

All the building blocks as well as entire data infrastructure must also be in aligned with Ayushman Bharath Digital Mission. This mission forms the basis for April, 2022 Health DataManagement Policy which must also be complied with by the data infrastructure. The policy in brief lays down r\the following as the framework for data fiduciaries[6]:

- The Data Principal must all points in time have control and decision making powers with respect to all the data collected from him as well as all the manners in which his data can be accessed or even processed.
- A fool proof mechanism to obtain digital consent satisfying both national and international standards.
- The disclosure or sharing of personal data must be seamless across all platforms, be it through any device, application or operating system i.e. interoperability must beensured.
- The data fiduciary also has the responsibility to check whether the consent he has received from the data principal is valid prior to collecting the data.
- The standards set for identifying validity of consent are as follows[7]:
    a. It must satisfy the basics rules laid down in Section 14 of Indian Contract Act
    b. The scope of the consent given by the data principal must be clearly enunciatedto the data principal.
    c. Data Principal has both the powers to give consent as well as withdraw his consent.
    d. It is essential that the process for withdrawing consent must be as simple as the process for obtaining consent – data principal must not be forced to undergo a cumbersome procedure for withdrawal process.
    e. It is also mandated that the collection as well as processing of personal data must be in conformity with the list of purposes authorised by National Health Authority.
    f. In scenarios wherein processing of data might result in severe or significant harm to the data principal, the same must be very explicitly stated to the data principal before obtaining his consent for all such sensitive information being collected and processed.

4.1. S.14 of Indian Contract Act

4.2. Privacy Notice- Scope of Consent

While obtaining consent from the data principal clear cut notice must be provided

- Prior to collection of data.
- Anytime data fiduciary changes privacy policy or procedures – thus a fresh consent isrequired every time there is a change.
- Any time data is collected for processed previously unidentified / new purpose – fresh consent is required.

The privacy notice must contain the following details[8]:

- The purpose for which the data is collected must be clearly indicated.
- The nature and category of data collected must be specified.
- Mechanism through which data is collected must also be specified.
- The identity and contact details of the data fiduciaries who are collecting the data mustbe mentioned.
- The period / criteria on basis of which the data so collected, will be retained must alsobe clearly laid down.
- It is also mandated that the privacy notice must be easily comprehensible and also available in all the languages in which the data fiduciary is intending to provide services.

4.3 How to obtain consent?

The consent can be obtained electronically or physically, from the data principal or the Health Information Exchange Consent Manager. In cases where consent is obtained physically, the same must be converted to electronic format by the Consent Manager / Data Fiduciary. Whereas in cases where the consent was obtained digitally through the Consent Manager itself,the Consent Manager:

- Must not access process or store any data shared with data fiduciary based on theconsent so received.
- Must maintain a record of all consents received as well as revoked
- Maintain a log of consents received as well as withdrawn for audit purposes.
- Whenever consent is revoked by the data principal, the same must be intimated by theconsent manager to all data fiduciaries concerned.

4.4 Rights of Data Principals[9]

The data principal can request for confirmation as to whether any of his personal data has been processed. These requests can be made both in writing as well as through any approved electronic methods including emails to the designated officer appointed by the data fiduciary. When such a request is made the

[6] *Ministry of Health and Family Welfare, Government of India (2022.) Draft Health Data Management PolicyVersion 02, Pg. 11, Retrieved from: https://abdm.gov.in:8081/uploads/Draft_HDM_Policy_April2022_e38c82eee5.pdf*

[7] *Ibid*

[8] *Ibid, Pg. 11,12.*

[9] *Ibid, Pg. No. 14.*

data principal must be made aware if any such processes have been applied as well as informed about the summary of such processes. The data principal also has a right to know the list of data fiduciaries who can access their data, this information must be readily available to them in a single page in an easily understandable format. The data principal must also have a mechanism through which he can restrict or object to disclosure of his personal data in conformity with existing laws. The data principal also has a right to request that his data be transferred to some other data fiduciary - i.e. data portability right is provided. In scenarios wherein the request is rejected, the reasons must be given by fiduciary. If the data principal is unsatisfied the same must be indicated by the fiduciary along with the datathat is to be displayed as well as nature of the dispute when the data record is accessed. A list of requests received by the data fiduciary must be also be properly maintained, even if the requested are denied.

4.5 Obligations of Fiduciaries Vis-à-vis Data Privacy

The data fiduciaries have an obligation to comply with data privacy policies when it processes any personal data, however it is also to be understood that the true control over dataresides with the data principal. Data fiduciary are liable only to the extent of proper executionof privacy policy with respect to the data that is in their repositories. The data fiduciary must also display the procedure to be followed by the data principals both for exercising their rights,as well as registering complaints seeking to redress the same. Fiduciaries also have to ensure that there is transparency with respect to categories of data collected as well as the manner andpurpose of collecting such data. All this information must be submitted to the National HealthAuthority as part of the annual report submission.

The federated system envisioned by the Blueprint ensures that no personal data other than what is required at a bare minimum to create and maintain Unique Health ID – AyushmanBharath Health Account [ABHA] can be stored. ABHA is to be created using KYC procedures using AADHAR / PAN Card/ Driving License/ Passport /any other digital system or documentspecified by the National Health Authority[10]. The data fiduciary is also mandated to prepare a privacy policy and prominently displaythe same in their websites. It must contain information regarding[11]:

- Practices and policies that will be followed by them.
- Types of personal information collected, manner as well as purpose for whichit is collected.
- Technical systems and business practices followed to identify anticipate andavoid harm to data principal.
- The standard and type of technology they are planning to use to process data.

The data must not be retained by the fiduciary beyond the time period indicated by thepurpose for which it was collected. The fiduciary is also mandated to conduct periodic reviewto determine whether they need to continue to possess and store the data so collected by them as per the laws applicable. The data must not be store beyond the geographical boundaries of India, to ensure that they are always subjected to Indian jurisdiction and privacy laws. The fiduciary is mandated with the following also:

- Ensure that the data is protected by them as well as its authenticity is validatedby them.
- In case of any data breach same must be intimated to the data principal as wellas National Health Authorities. They may also be called upon to showcase the security measures implement by the to protect data.
- Must have a mechanism to protect the integrity of the data collected, prevent unauthorized retrieval, disclosure, modification or deletion of private data.
- The Chief Information Security Officer [ABDM CISO] and the Data Protection Officer [ADBM DPO] are empowered to do periodic review of all the security safeguards implemented by the data fiduciary.
- The fiduciaries will also be required to undergo audit by independent agenciesapproved by the government once a year or every time there is a significant upgradation of its systems or software.

5. LEGAL AND PRACTICAL CONCERNS

It is globally recognised that patients have right to privacy, thus they are to a great extent capable of determining if their health information is to be withheld or disseminated to select few on basis of their discretion or the public at large. Few exceptions to this rule will always rely upon public health concerns, such as information pertaining to an HIV patient beingreleased to their future spouse to make informed decision or information relating to being affected by a severe contagious disease requiring quarantine. In many research scenarios the law requires that when data is shared it must be de-identified data so that data cannot be tracedback to the data principal. Eg: A researcher will only need the number of patients affected by HIV in a particular locality and not their specific identities. Apart from the above mentioned scenarios it is well recognised that a patient has right to privacy as well as confidentiality when he opts for clinical interactions which cannot be easily disregarded in face of digitalisation. The relationship that exists between a doctor and his patient is fiduciary in nature and communication privileged in sense that it is confidential. The same was recognised in India in many cases including the ***Shri Shravan Kumar V Ihbas,New Delhi 2009*** case[12]. In this case, information was denied to the husband of a psychiatric patient when requested under RTI Act, stating that the information sought is personal information held in a fiduciary relationship by the doctors in the institution. The digital health policies ensure that the data principal is always protected by the concept of informed consent as well as providing a way to opt-out if they wish to. While announcing that the pilot phase of national digital health id under NDHM, Minister of State forHealth Ashwini Chowbey pointed out that there are no data privacy concerns as collection of data is based upon the consent of the individual. He also stated that, the pilot phase of missionis active in Andaman &

[10] *Ibid, Pg. No 15.*

[11] *Ibid, Pg. No 20,21.*

[12] *CIC/AD/C/2009/000233, Para 6, https://indiankanoon.org/doc/1396043/*

Nicobar, Dadra & Nagar Haveli, Diu & Daman, Ladak, Lakshwadeep and Puducherry alone[13]. The G.Os issued by Puducherry government in this respect includes G.O issued by Directorate of Higher and Technical Education on 12/1/2021 and Directorate of Health and Family Welfare Services issued on 9/1/2021. A basic read of The Directorate of Higher and Technical Education orders lays down[14]:

- Direction that students of all higher Educational Institutions as well as their parents must be informed that they need to create National Digital Health ID.
- Direction that a nodal officer needs to be identified and appointed by each college. Thisnodal officer needs to ensure that 100% registration of students and their family members are completed.
- The nodal officer also needs to submit a compliance report that the registration is completed as per direction to the Directorate of Higher and Technical Education.
- The Head of Institutions are further directed that from the upcoming year the health IDof the student must be displayed in the Student ID card.

A basic read of The Directorate of Health and Family Welfare Services orders also mandates the same points as listed above[15]. A bare read of the two circulars makes it crystal clear that they stand in violation of the various digital health policies laid down by the government. All the health ID creation policies articulates and mandates the concept of informed choice coupledwith that of the right to 'opt-out'. Both these GOs are calling for 100% registration and doesn'teven highlight the fact that the citizens have a choice to not register for Digital Health ID. Thepilot project itself failing to follow the mandate of Digital Health policy seems to set an alarming trend, which needs to nixed in the bud itself. The other worrisome aspect highlighted by various news portals such as India Today and Scroll.in is about the fact that Health IDs are created even with people registering for the same. Scroll.in as a part of its investigative journalism points out to various cases wherein manycitizens found out that they had a Digital Health ID simply because they had used the CoWin app to register for and avail Corona Vaccines[16]. India Today[17] also found out similar such occurrences and went further ahead to point out that when citizens volunteer to create health idthrough the NDHM website they are refused the same as only the pilot project is running for few select locations. This goes to show case that many citizens who are having Health IDs didnot obtain it by way of self-registration rather the same was done by some intentional / non- intentional glitch in the system that generates health ids based on registration for vaccine through CoWin app. This news article also points out to the alarming lack of concern regardinginformed consent. Even if the glitch is unintentional it cannot be simply ignored at wished away. The directions of GOs also violates the S.C. ruling in Puttuswamy case[18] whichguarantees the right of an individual 'to be let alone' which forms the crux of informed consent. One of the reasons why there is apparent lack of concern about informed consent, couldbe based on that fact that we lack stringent laws inspite of clear guidelines laid down in the digital health policies. In Puttuswamy case[19] SC has mandated that there is a need for data protection laws. In this case Dr. D. Y. Chandrachud. J. observed that there danger for privacy in this information age can arise both from State as well as Non-State actors, thereby creating a need for 'robust regime for data protection.[20]' In the same case, Justice S.K. KAul reitreated the same when he observed that there is an 'unprecedented need to regulate the extent to which such information can be stored, processed and used by non-State actors.[21]' ·Even though the government has taken steps to bring out data protection laws, there hasbeen no concrete enactment until The Digital Personal Data Protection Act, 2023 was broughtout. The earlier Data Protection Bill, 2021 was withdrawn from Lok Sabha on 3/8/2022[22]. The reasons cited by Minister of State for Information Technology Mr. Rajeev Chandrashekar was that the Joint Committee of Parliament, had called for 81 amendments and

---

[13] No violation of data privacy under National Digital Health Mission, Rajya Sabha told. The Economic Times.(2021, February 2). Retrieved from https://economictimes.indiatimes.com/news/politics- and-nation/no- violation-of-data-privacy-under-national-digital-health-mission-rajya-sabha- told/articleshow/80649481.cms.

[14] The Directorate of Higher and Technical Education. (2021). Creation of Health IDs for All College Students and their Families. No. 2971/DHTE/Tech./T3/2021. Retrieved from https://dhte.py.gov.in/viewpdf?url=0&nid=2274

[15] The Directorate of Health and Family Welfare Services. Creation of Health IDs for All College Students andtheir Families. No. 13/DHFWS/PA/2021. Retrieved from https://dhte.py.gov.in/viewpdf?url=0&nid=2274

[16] Barnagarwala, T. (2022, August 27). How India is creating digital health accounts of its citizens without theirknowledge. Scroll.in. Retrieved from https://scroll.in/article/1031157/how-india-is- creating-digital-health- accounts-of-its-citizens-without-their-knowledge

[17] Dogra, S. (2021, May 24). Took covid vaccine using Aadhaar? your national health ID has been created without your permission. India Today. Retrieved from https://www.indiatoday.in/technology/features/story/took-covid-vaccine-using-aadhaar-your-national-health- id-has-been-created-without-your-permission-1806470-2021-05-24.

[18] Justice K.S.Puttaswamy (Retd) vs Union Of India (Supreme Court of India September 26, 2018). AIR 2017 SC 4161, (2017) 10 SCC 1. Retrieved, from https://indiankanoon.org/doc/127517806/.

[19] Ibid.

[20] Ibid, Para 328.

[21] Ibid, Para 591.

[22] Joshi, K. (2022, August 3). Centre withdraws personal data protection bill, 2021 from Lok Sabha; New Law Soon. Republic World. Retrieved from https://www.republicworld.com/india-news/politics/centre- withdraws-personal-data-protection-bill-2021-from-lok-sabha-new-law-soon- articleshow.html

12 recommendations[23]. The government as promised adopted the new data protection lawin 2023. The new enactment is yet again riddled with various issues including:

- It allows the data fiduciaries to collect data for legitimate purposes, but fails to clarify how long the data can be retained and whether the data so collected can be used to track preferences of a person.
- When data is collected by the instrumentality of the government specifically for health aspects, the powers of such entity is very vast. The reference line given is that these instrumentalities of the State must follow the guidelines and policy of the Central government in this case.
- Though the Act speaks eloquently about informed consent, it provides no mechanism through which the common man is made aware of his rights. There is a need for bringing out a state-based advocacy group to ensure common man is aware he has a right of informed consent.
- The Act also talks about need to take reasonable security precautions against data breach, but rather ambiguous as to the standards for reasonable precautions. A Principal can complain to the Data Protection Board, which will then conduct the enquiry as under

S.33. Even though personal data breach can involve a levy of penalty up to Two Hundred and Fifty crore rupees, the Act stands silent about the right of the data principal to claim compensation. S. 34 very clearly mandates that, all sums realized by way of penalties imposed by the Board under this Act, must be credited to the Consolidated Fund of India. Apart from all these legal issues, there is also a need to train Health Information Management [HIM] Professionals, otherwise the entire health data infrastructure will collapse. India faces acute shortage of trained professionals capable to efficiently capture information, which is a major drawback that needs to be promptly addressed. In fact, it has been pointed out that both the institutions a curriculum that addresses this issue is very low[24].

6. CONCLUSION

These states of affairs simply telecast that India is not yet ready with robust data protection mechanisms and laws. This state of affairs simply telecast that India is not yet readywith robust data protection mechanisms and laws. The Digital Personal Data Protection Act, 2023 also fails to translate the mechanisms aid down in the Health Policies into legal realities. The infrastructure that is there in the Digital Health Vision must translate as ground reality incorporating privacy concerns of the common man. Clarity to the executives, regarding implementation of the Digital Health Mission is also very much required. Training regarding informed consent needs to be done properly to ensure no such fiascos occur in future. Of equal import is the need to educate the common citizens regarding their rights. Thus, even though the entire framework, policies and enactment look well put in paper there is a need to ensure that the same is faithfully translated into practice, without any slips or modifications.

7. CONFLICT OF INTEREST

Conflict of interest declared none.

[23] The Economic Times. (2022, August 4). Govt withdraws data protection bill, 2021. The Economic Times. Retrieved from https://economictimes.indiatimes.com/tech/technology/govt-withdraws- data-protection-bill-2021/articleshow/93334281.cms?utm_source=contentofinterest&utm_medium=text&utm_campaig n=cppst

[24] Gudi, N., Lakiang, T., Pattanshetty, S., Sarbadhikari, S. N., & John, O. (2021). Challenges and prospects in india's digital health journey. Indian journal of public health, 65(2), 209–212. https://doi.org/10.4103/ijph.IJPH_1446_20