Comments on the National Digital Health Blueprint

August 04, 2019

Authored by **Samyukta Prabhu, Ambika Tandon, Torsha Sarkar** and **Aayush Rathi**

with inputs from **Amber Sinha**

The Centre for Internet and Society (CIS), India
https://cis-india.org

Designed by Saumyaa Naidu

General Comments

This submission presents comments by the Centre for Internet and Society (CIS), on the National Digital Health Blueprint (NDHB) Report, released on 15th July 2019 for public consulations. It must be noted at the outset that the time given for comments was less than three weeks, and such a short window of time is inadequate for all stakeholders involved to comprehensively address the various aspects of the Report. Accordingly, on behalf of all other interested parties, we request more time for consultations.

We also note that the nature of data which would be subject to processing in the proposed digital framework pre-supposes a robust data protection regime in India, one which is currently absent. Accordingly, we also urge ceasing the implementation of the framework until the Personal Data Protection Bill is passed by the parliament. We would be explaining our reasonings on this particular point below.

Introduction

The National Digital Health Blueprint (NDHB) references both the government's commitment to bring about universal health care (UHC) as well as the two-pronged healthcare system unveiled last year, Ayushman Bharat Yojana (ABY) in its preliminary statement, with the underpinning assumption that implementation of the NDHB will aid both.

In our previous comments on National Health Stack (NHS) last year, we had drawn a comparison between the NHS and the NPfIT, the UK government's attempt to digitize its healthcare service. The latter's failure to achieve its objectives spurned considerable amount of literature, pointing out that any digitization in the healthcare sector should be done with three aims in mind - better health, better healthcare and lower costs.[1] This being said, it is useful to consider the NDHB's assumption briefly, and see whether the existing ground realities support it.

Health insurance in India

Previous experiences with government-sponsored health insurance schemes have proven that there is little merit to such an expensive task. The Rashtriya Swasthya Bima Yojana (RSBY), for instance, which covered thirty-three crore people witnessed a substantial

[1] Report of the National Advisory Group on Health Information Technology in England, 'Making IT Work : Harnessing the Power of Health Information Technology to Improve Care in England', available at <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/550866/Wachter_Review_Accessible.pdf >

increase in out-of pocket (OOP) expenditures[2], which is also the cause for around fifty million Indian households falling annually into poverty.[3]

An interplay between three factors offset the government's efforts to provide UHC - a) the service of healthcare captured by the private sector, b) a higher amount of private expenditure, as opposed to public expenditure and c) paucity of public services, due to the dilapidated state of public health sector.[4]

Additionally, these traditional insurance-based models are characterized by problems of information asymmetry, like moral hazard. In this case, patients and healthcare providers have no incentive to control their costs and tend to overuse, resulting in an unsustainable insurance system and cost inflation[5]. Any attempt to regulate providers is met with harsh, cost-cutting steps which end up harming patients[6].

In our previous submissions for the National Health Stack (NHS) last year, we had pointed out that the Indian socio-economic realities of healthcare were inadequate to support the aims of the ABY. We continue to maintain that opinion, and the full versions of the comments are available online. In view of the persisting socio economic inequalities in the Indian healthcare sector therefore, it is our opinion that mere digitization of healthcare sector, as envisaged in the NDHB, would not serve any increment in the quality of care available to the people.

Lack of institutional knowledge and capacity

Earlier iterations of health information systems in India have suffered from incomplete data due to lack of knowledge and clarity among health workers. Such initiatives, including the HMIS and MCTS/RCH, have also suffered from lack of capacity as overburdened health workers and data entry operators are unable to devote adequate time to health information systems[7]. The PHR will be in addition to all such existing databases that are geared towards specific goals, resulting in greater workloads. Inadequate capacity has also led to long gaps between the event and the digitisation of relevant data[8], which could also be a cause for concern in the NDHB as data may not

[2] Ravi Duggal, 'Health Insurance Companies Will Definitely Gain, But Can We Say the Same for the Poor?', (*The Wire,* 6 February, 2018)
<https://thewire.in/economy/health-insurance-budget-2018-nhps> accessed 4 August 2019.
[3] Sanjay Zodpey and Habib Hasan Farooqui, 'Universal Health Coverage in India: Progress achieved & the way forward', (2018) 147(4) Indian Journal of Medcial Research
<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6057252/> accessed 4 August 2019.
[4] Id.
[5] Sheetal Ranganathan, 'National Health Protection Scheme will not help its intended beneficiaries' (*Livemint*, 15 February 2018)
<https://www.livemint.com/Opinion/k80NvWWKvFGwHptVIDIqNJ/National-Health-Protection-Scheme-will-not-help-its-intended.html> accessed 4 August 2019
[6] G. Ananthakrishnan, 'Regulating India's regressive health insurance' (*The Hindu*, 22 February 2017)
<https://www.thehindu.com/sci-tech/health/policy-and-issues/Malady-Nation-Regulating-India%E2%80%99s-regressive-health-insurance/article14564554.ece> accessed 4 August 2019.
[7] Madhulekha Bhattacharya, Renu Shahrawat, and Vinod Joon (2012). Understanding Level of Maternal and Child Health Indicators used in Health Management Information System among Peripheral Level Health Functionaries in Two Districts of India. *Journal of Health Informatics in Developing Countries*, 6(1).
[8] Ramkrishnan Balakrishnan, Vijayaprsad Gopichandran, Sharadprakash Chaturvedi, et al. (2016). Continuum of Care Services for Maternal and Child Health using mobile technology – a health

necessarily be digitised at source. The NDHB envisions that existing systems will be made interoperable with the NDHE, which will imply changes in the functioning of these systems. Data entry operators will then be burdened with relearning these processes as well as adapting to the PHRs. These issues have also resulted in an overemphasis on data collection in health information systems in India, and not enough capacity for analysis and planning locally[9].

While the NDHB does address this issue through the principle of minimization, this will not be enough to incentivize and standardize the use of the NDHE. We recommend a strong focus on capacity building, training, and additional resource allocation as part of the implementation plan of the NDHB, especially in resource poor settings that suffer from poor connectivity, regular electricity, and other infrastructural constraints. We further recommend a focus on local use of data for planning of health services across different health information systems.

Specific comments

The assumption of 'near universal coverage' of smart phones

The NDHB also assumes that access and delivery of the services promised under the ecosystem would be facilitated by the prospect of 'near universal coverage' of smart phones across India. However, this 'mobile first' premise rests on an assumption of widespread digital literacy, which is simply absent when one considers the social realities of the country. In a recent report, the Digital Empowerment Foundation revealed that nearly ninety percent of the population are not digitally literate[10] despite the country being the second fastest-growing market for mobile phones.[11] Moreover, the GSMA mobile penetration report for 2018 notes a 23 percent gender gap in ownership of mobile phones

system strengthening strategy in low and middle income countries. *BMC Medical Informatics and Decision*

[9] Study of Public Health IT Systems in India Background Study for ICT subgroup of Sector Innovation Council in Health. (2019). [online] New Delhi: National Health Systems Resource Centre and Taurus Glocal Consulting. Available at: http://nhsrcindia.org/sites/default/files/Public%20Health%20IT%20Systems%20Study%20NHSRC_0.pdf

[10] 'A look at India's deep digital literacy divide and why it needs to be bridged', (*Financial Express*, 24 September 2018) <https://www.financialexpress.com/education-2/a-look-at-indias-deep-digital-literacy-divide-and-why-it-needs-to-be-bridged/1323822/> last accessed 4 August 2019

[11] Information extracted from the website of National Digital Literacy Mission

- only 63 percent women in India own mobile phones[12]. These issues have also plagued earlier mHealth initiatives, such as the Mother and Child Tracking System[13].

In such light, it becomes difficult to understand the rationale of the document in making internet connectivity as an exclusive, essential background condition for widespread delivery of healthcare. If the framework continues to emphasize the existence of a smartphone as a prerequisite to a citizen effectively enjoying the benefits of the PHR, then it would only act as an exclusionary barrier to access for the large number of population who lack either a mobile phone or internet connectivity.

We recommend a focus on digital access and literacy, especially for underrepresented populations, simultaneously with the implementation of the NDHB.

Standards for Content and Interoperability

Part (a) of the Section on interoperability in the NDHB, pertaining to technical interoperability, contains a recommendation for a federated architecture for collecting and storing health information. However, it does not clearly demarcate categories of data that will be stored in regional centres or at the sites of service providers, versus those categories that will be stored in the Central Repository of NDHB. It states that "a bulk of the information relating to citizen/patient health records" would be managed in a distributed model. This does not clarify what categories of personal health records, if any, will be stored in the Central Repository, in regional centres, or at individual service centres. It also does not specify a process by which this will be determined.

It is also unclear how the Consent Manager will ensure that each PHR is in control of the data principal while being stored at each of these different sites, or enforce the use of the recommended standard ISO/TS 17975:2015. Additionally, while the focus on open standards and interoperability is commendable, it is far more difficult to operationalise the interoperability given the array of open standards to choose from. Often, in the case of decentralised personal data stores, interoperability then gets reduced to the use of open standards.[14] This will get amplified in the context of an extremely complex system like that proposed in the NDHB as the parameters to be handled grow exponentially with increased use. This promises to pose a serious challenge for software and hardware developers and may even require working with standards setting organisation.

We recommend that there be greater clarity on the categories of data to be stored at different sites in the federated architecture, as well as the process for ensuring the consent of the data principal for data capture and data use. Additionally, a specific plan ensuring the interoperability of standards to be used needs to be devised.

---

[12] GSMA, 'The Mobile Gender Gap Report 2018' <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/04/GSMA_The_Mobile_Gender_Gap_Report_2018_32pp_WEBv7.pdf> last accessed 4 August 2019

[13] Pallavan Nagarajan, Jaya Prasad Tripathy and Sonu Goel (2016). Is mother and child tracking system (MCTS) on the right track? An experience from a northern state of India. *Indian Journal of Public Health*, 60(1), p.34.

[14] Narayanan A, Toubiana V, Barocas S, Nissenbaum H, and Boneh D, "A Critical Look at Decentralized Personal Data Architectures," Data Usage Management on the Web

Possible failure of Anonymization/De-identification

The Srikrishna Committee's Data Protection Committee Report has commented on the possibility of failure of methods of de-identification/anonymisation.[15] This is because quasi-identifiers[16] may be used to link seemingly anonymised data to the respective individual. It is important to note here that some jurisdictions such as the EU and South Africa[17] have put anonymised data outside the scope of data protection law. While India has similar provisions in the Personal Data Protection Bill 2018, [18], it also has an additional provision of criminalisation of de-identification of anonymised data, without the consent of the data fiduciary.

As recommended by the Data Protection Committee Report,[19] the Data Protection Authority (DPA) should *create these standards that the health data under NDHB should follow*, to ensure the privacy of individuals.

As recommended in CIS's comments[20] on the Electronic Health Records (EHR) to address quasi-identifiers, we could borrow from the definition and scope of Protected Health Information under HIPAA to *include identifiers such as Device identifiers and serial numbers, Web Universal Resource Locators (URLs), Internet Protocol (IP) address numbers*, in addition to other general "personally identifiable information" about an individual.

The NDHB says "[...] Anonymizer enables the Government or authorized agencies may need to access the health records of the citizens especially in some identified cases like monitoring of notified diseases etc., to take effective decisions to promote wellness in the country and to ensure that healthcare is provided in a timely fashion, as needed." To address the possible failure of anonymisation of data, we recommend that the NDHB include an exhaustive list of bodies/individuals that can gain access to this anonymised data and a list of identified cases wherein they can do so. This is to ensure that anonymised data is only accessed by authorised agencies as specified by the Government. This should consider the recommendations made in the MoHFW's Draft Digital Information Security in Health Act (DISHA) bill, which includes "*Digital health data, whether identifiable or anonymized, shall not be accessed, used or disclosed to any person for a commercial purpose and in no circumstances be accessed, used or disclosed to insurance companies, employers, human resource consultants and pharmaceutical companies, or any other entity as may be specified by the Central Government.*"[21]

---

[15] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna [*hereinafter Srikrishna Report*]<https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf>

[16] "*Quasi-identifiers are 'pieces of information representing a person's background information (e.g. their date of birth, clinic visit, residence postal code, sex and ethnicity) that are not of themselves unique identifiers but which can be combined with other quasi-identifiers and become personally identifying information'.*" Data anonymization - a key enabler for clinical data sharing" <https://www.ema.europa.eu/en/documents/report/report-data-anonymisation-key-enabler-clinical-data-sharing_en.pdf> accesed 4 August 2019.

[17] Srikrishna Committee Report []

[18] Personal Data Protection Bill 2018, Section 2(3).

[19] Srikrishna Committee Report [n]

[20] Amber Sinha, "Comment on the Electronic Health Records Standards", *Centre for Internet and Society*
<https://cis-india.org/internet-governance/blog/comments-on-draft-electronic-health-records-standards> accessed 4 August 2019

[21] Draft Digital Information Security in Health Act Bill
<https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf> accessed 4 August 2019

The DISHA bill 2018, in Chapter 4 (31) specifies that the individual themself owns their digitised health data. One possible recommendation could be that the NDHB report borrow from DISHA (in case DISHA is not passed to be an Act) to include ownership rights by the individual.

Additionally, the NDHB also does not clarify whether the anonymised data can be accessed by citizens through the Right to Information, in the case that it is not owned by the individual and is owned by the state.

Consent Framework Recommendations

Although the NDHB recommends the usage of certain consent frameworks, there are two points that need to be kept in mind for successful implementation. Firstly, that around 90% of the Indian population is not digitally literate[22], furthermore, about 30% of the population is illiterate. Secondly, as acknowledged by the Srikrishna Committee's Data Protection Committee Report, that there is a widespread presence of boilerplate contracts in the online world,[23] which may not be read and/or understood by most people who consent to it. Keeping these two points in mind, there is a need to develop a revised consent framework that allows the citizens to give informed and explicit consent regarding capture and use of their health data.

For this, the Srikrishna Committee recommends a 'revised framework of consent' as borrowed from Arthur Leff in his article 'Contract As Thing', who proposes that contracts be treated as a product.[24] This introduces the regime of product liability, which means that data fiduciaries will be liable as if the consent form was a product.[25] The data fiduciaries would have obligations to "provide active consent frameworks to data principals in a manner that they do not escape the attention of the latter [data principals]."[26] The paper further specifies other substantive obligations such as "showing notice before any such practices communicated in the notice take place",[27] "requiring affirmative consent from the data principal without any pre-checked boxes"[28] and "providing requisite granularity thereby allowing data principals to access services without necessarily consenting to all or nothing."[29]

In summary, we recommend that the consent management framework be implemented in a manner that takes into consideration the presence of significant number of citizens that are digitally or otherwise illiterate. In order to ensure that they provide informed and specific consent with respect to their digital health data, consent forms be treated like a product, subject to product liability. The data fiduciaries are then obligated to design consent contracts/frameworks such that there are no pre-checked boxes or boilerplate contracts. They are required to design them in a manner such that they are read and understood by the data principals, thus allowing the latter to provide informed, affirmative consent.

---

[22] Financial Express [n]
[23] Srikrishna Committee Report [n]
[24] Id.
[25] Id.
[26] Id.
[27] Id.
[28] Id.
[29] Id.

Privacy gaps and other issues with HealthLocker and eSign Framework for Aadhaar

A CIS report on "Privacy Gaps in India's Digital India Project"[30] outlines the privacy gaps in schemes such as DigiLocker (which HealthLocker will be modeled upon) and eSign framework for Aadhaar. These include the following:

- For DigiLocker, the inadequacy of security measures provides privacy threats to biometric data that is stored in it.[31] If the same measures are implemented in the HealthLocker, the privacy threat is further increased due to the presence of sensitive health data. Additionally, there is no method to take explicit consent from the users of DigiLocker -- the consent is assumed when individuals sign up for the service.[32] We recommend that explicit consent be taken from users in HealthLocker. Additionally, the consent layer in the National Health Stack will only be meaningful if the requirement of explicit and affirmative consent is built into the design of the product.
- For eSign framework for Aadhaar, despite the presence of security measures, there exist security concerns due to the involvement of private third parties.[33] We recommend a transparent and rigorous vetting process for third parties involved, as well as strict access limitations for all third parties.

Recommendations on the use of Personal Electronic Health Records

Central to the implementation of the NDHP also is its focus on personal electronic health records (PHRs). While it is unclear what shape PHRs will take under the NDHP, PHRs are widely associated with several benefits that include health self-management and the simultaneous empowerment of patients, better access to information that improves communication between patients and providers.[34]

However, evidence suggests that these benefits only accrue to technically competent users.[35] In addition to digital literacy, then, the effective use of PHRs is contingent on health literacy. Health literacy in most low to middle-income contexts is quite low, and India is no exception.[36] This will stand to have implications on both the adoption and use

[30] Anisha Gupta, "Privacy Gaps in India's Digital India Project", *Centre for Internet and Society*, <https://cis-india.org/internet-governance/files/digital-india-report.pdf> accessed 4 August 2019.
[31] Id.
[32] Id.
[33] Id.
[34] Tang PC and Lansky D, "The Missing Link: Bridging The Patient–Provider Health Information Gap" (2005) 24 Health Affairs 1290; Pagliari C, Detmer D and Singleton P, "Potential of Electronic Personal Health Records" (2007) 335 BMJ 330
[35] Ralston JD and others, "Patient Use of Secure Electronic Messaging Within a Shared Medical Record: A Cross-Sectional Study" (2009) 24 Journal of General Internal Medicine 349
[36] The World Health Organisation, "Health literacy key to improving health outcomes in South East Asia" <http://www.searo.who.int/entity/healthpromotion/events/health_literacy_book_launch_2014/en/> accessed 4 August 2019

of PHRs as any benefits accruing through PHR use are contingent on the frequency with which they are used.

Those that stand to lose out on the use of PHRs then stand to be communities that are already underserved in the delivery of health services. For these underserved communities, the risk of exclusion already exists in part to the difficulties inherent to delivering care in remote locations, barriers related to cross-cultural communication, and the pervasive problem of providing care in the setting of severe resource constraints. Equally as important, health workers already report significant constraints to delivering routine care in these settings, and may view electronic health records as having limited value in addressing the particular needs of their patient population.[37]

Additionally, the benefits accruing from PHR use are also closely tied to the use of EHR systems by health care providers. Importing the success of these electronic health programs from other high-income contexts does not factor in the endemic reasons for clinicians' inertia in the adoption of EHRs. For instance, there is a wide disparity in low and middle-income contexts vis-a-vis high income contexts.[38] As a result, doctors in India tend to be more problem-oriented, time-strapped, and pay less attention to the elaborate documentation of clinical notes.[39]

In a similar vein, the funding requirements for a nation-wide EHR program are best highlighted through the results of a WHO survey studying the global implementation of EHRs: wealthier countries were overrepresented with two thirds in the upper-middle income group and roughly half of high-income countries having introduced EHR systems, while a third of lower-middle-income countries and 15% of low-income countries reported having implemented them.[40]

The Standards for Privacy and Security in the NDHB refer to the EHR Standards for India 2016 for more information. In a CIS report[41] regarding Comments on Draft EHR Standards, a few recommendations were proposed that we continue to recommend. These broadly include the following:

- That all personal health records (which includes medical records as well as administrative healthcare records such as information about enrollment, payment etc.) be deemed to be owned by the patient.[42] Additionally, the NDHB rationalizes the existence of a Consent Manager to ensure that the Data Principal is in complete control of what data is collected, how it is shared, for what purpose and how it is shared. While this is commendable, we recommend that the NDHB clarifies that this Consent Manager would ensure the same set of rights for anonymised data as well.
- The EHR standards do not mention a duration within which healthcare providers must provide required information to individuals. A time-limit such as 30 calendar

[37] Rathi A and Tandon A, "Big Data and Reproductive Health in India: A Case Study of the Mother and Child Tracking System" The Centre for Internet and Society (Forthcoming)
[38] https://www.who.int/gho/health_workforce/physicians_density/en/
[39] Kandhari, R, "Why a backdoor push towards eHealth" The Ken <https://the-ken.com/story/why-backdoor-push-towards-ehealth/> accessed 4 August 2019
[40] The World Health Organisation, "Global diffusion of eHealth: Making universal health coverage achievable" <https://apps.who.int/iris/bitstream/handle/10665/252529/9789241511780-eng.pdf;jsessionid=9DD5F8603C67EEF35549799B928F3541?sequence=1> accessed 4 August 2019
[41] Amber Sinha [n]
[42] Id.

days was recommended, within which the healthcare provider must process the request.[43]
- All bodies dealing with medical data should be required to abide by the principle of data minimization in use and disclosure.[44]
- For internal uses, healthcare providers and other entities must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of their workforce.[45]

Risks and issues regarding Government Community Cloud

The Government Community Cloud, that is, the GI Cloud (Meghraj) has several risks and issues mentioned in its Strategic Decision Paper,[46] such as "risk of compromise of confidential information and intellectual property."[47] It also mentions that cloud based application design varies significantly from traditional application design.[48] If healthcare systems are to be standardised across India, there will be high costs involved. We recommend that the costs involved in the project be laid out in significant detail before any steps to implement the same.

Right to Forget in the Personal Health Records

Section 3.5 of the NDHB states the standards that will be in place for privacy and security, which includes provisions that are to be included in the operational aspects. This includes a provision on immutability, which states that a record cannot be deleted without following due process.

We recommend that such due process takes into consideration the right of the data principal to delete specific entries or the entire set of records containing their personal information. We had also made this recommendation for the Digital Information Security in Healthcare Act 2018[49], and reiterate it for the NDHB.

Responding to data and privacy breach

The NDHB does not contain any mention of the procedure to be followed in case of a data breach. While it does recommend the creation of a Security Operations Centre (SOC) and a NDHB Security Policy, it does not deal with the procedure to be followed by the SOC or

[43] Id.
[44] Id.
[45] Id.
[46] Department of Electronics and Information and Technology, "Government of India's GI Cloud (Meghraj) Strategic Direction Paper" <https://meity.gov.in/writereaddata/files/GI-Cloud%20Strategic%20Direction%20Report%281%29_0.pdf> accessed 4 August 2019
[47] Id.
[48] Id.
[49] Shweta Mohandas and Amber Sinha, "Comments on the Draft Digital Information Security in Healthcare Act", *Centre for Internet and Society* <https://cis-india.org/internet-governance/files/comments-on-draft-digital-information-security-in-healthcare-act> accessed 4 August 2019

each nodal centre in case of a breach of data or privacy at any level of the federated architecture.

We recommend the creation of a clear Standard Operating Procedure to be followed by each of the nodal centres and the SOC in case of a breach. We further recommend an emphasis on notifying the users who have been affected by such a breach, especially when pertaining to sensitive information.