Response to the Public Consultation on the draft Health Data Management Policy

IT for Change

September 2020

Table of Contents

1. Overview

In its statement of purpose, the draft Health Data Management Policy[1] declares its intent to serve as a guidance document on personal data protection across all dimensions of the National Digital Health Ecosystem (NDHE). It states that the secure, privacy-compliant ecosystem of network and cloud infrastructure, federated data hubs, application building blocks, technological standards and regulations that constitute the NDHE is intended to serve as the 'holistic' and 'interoperable' digital public infrastructure towards encouraging "*public and private innovation by providing the essential techno-building blocks (aggregate anonymised, non-personal health data sharing mechanisms and APIs) for the development of health service apps and health analytics solutions.*"

The National Digital Health Blueprint (the Blueprint) of the National Digital Health Mission (July 2020)[2] makes it clear that there are a range of associated policy frameworks – on Health IDs, data sharing, security, privacy and strategic control (outlined in Section 2.3 of the Blueprint) – that are collectively intended to address privacy, personal data protection and security considerations stemming from the NDHE. However, the draft National Health Data Management Policy has been released as a stand-alone document for this public consultation. To provide a holistic stocktaking of the Blueprint, it is essential for the public to have access to all the draft policies. This would allow for a close examination of the cross-policy elements, the overall framework guiding the digital health ecosystem, and if, and how, the policies are able to address the right to health[3] for all.

Under the circumstances, given that the draft Health Data Management Policy presents just one facet of the Blueprint, any assessment of it is bound to be partial, at best. Nevertheless, we would like to flag the following concerns from our reading of the document.

2. Privacy concerns arising from contravention of Puttaswamy judgment

The Government of India's decision to opt for a policy route to health data governance without a Personal Data Protection legislation and the rubric of sector-specific health data law is a cause for concern. In contravention to the law laid down by the Puttaswamy judgment,[4] the government is taking the route of delegated legislation and policy to affect privacy safeguards. Such practice is also in contravention of global good governance practices, as highlighted by the health minister of the state of Chhattisgarh.[5]

1 National Digital Health Mission. Health Data Management Policy. https://ndhm.gov.in/health_management_policy
2 Ministry of Health and Family Welfare, Government of India. (April 2019). National Digital Health Blueprint. https://www.nhp.gov.in/NHPfiles/National_Digital_Health_Blueprint_Report_comments_invited.pdf
3 It has been held that medical aid is a part of the fundamental right under Article 21. *CERC v. Union of India* 1995 SCC (3) 42.
4 *K.S. Puttaswamy & Anr. v. Union of India & Anr.* (2017) 10 SCC 1.
5 Scroll Staff. (2020, September 6). *New Health Data Policy may be Misused for Surveillance: Chhattisgarh Minister Writes to Vardhan.* Scroll. https://scroll.in/latest/972361/new-health-data-policy-may-be-misused-for-surveillance-chhattisgarh-minister-writes-to-vardhan

2.1. Conceptual ambiguities

i. Lack of clarity on key concepts pertaining to personal data protection.

The draft Health Data Management Policy defines some key concepts differently from the draft Personal Data Protection Bill (PDP Bill) (such as 'personal data,' 'anonymisation,' 'processing') while deploying other concepts from the PDP Bill without defining them (such as 'consent manager,' 'health data,' 'personal data breach'). This not only produces vagueness and arbitrariness in interpretation, but also does not address how any definitional ambiguity or conflict of terms with the final version of the PDP Bill, eventually enacted into law, will be resolved.

ii. Accountability of data fiduciary for valid consent not operationalised

The draft Health Data Management Policy adopts the PDP Bill's conceptualisation of consent as valid only when it is *"free, informed, specific, clearly given, and capable of being withdrawn any time."* Unfortunately, the draft Health Data Management Policy's consent framework fails to operationalise the PDP Bill's requirement of placing the burden-of-proof of valid consent directly on the data fiduciary.[6]

Further, Para 10.4 of the draft Health Data Management Policy, which details the process of furnishing a privacy notice as part of the procedure for obtaining consent only states that "*the privacy notice shall be clear, concise and easily comprehensible to a reasonable person and shall be available in as many languages in which the services of the data fiduciary are intended to be provided."* By limiting the obligation of data fiduciaries to merely issue the privacy notice in "*as many languages in which the services of the data fiduciary are intended to be provided,"* the obligation of data fiduciaries to ensure valid consent from a majority of individuals accessing health care services is minimised.[7] Evidently, this proviso does not ensure 'free and informed consent' in various circumstances of marginalisation; for instance, migrant workers accessing health care services in a destination state whose dominant languages they do not comprehend or individuals with no textual literacy/limited exposure to formal education.

2.2. Deficits in the proposed institutional governance mechanisms

i. No acknowledgement of the subordination of the NHA to the DPA

There is no express acknowledgement of the administrative jurisdiction of the Data Protection Authority (DPA) over the National Health Authority (NHA) in the provisions of the draft Health Data Management Policy. For example, the draft Health Data Management Policy does not specify

6 PDP Bill, 2019 (Section 11(5)).

7 "*Every patient has a right to adequate relevant information about the nature, cause of illness, provisional/ confirmed diagnosis, proposed investigations and management, and possible complications, to be explained at their level of understanding in language known to them. The treating physician has a duty to ensure that this information is provided in simple and intelligible language to the patient to be communicated either personally by the physician, or by means of his/her qualified assistants."* See: Charter for Patients' Rights for adoption by NHRC. http://clinicalestablishments.gov.in/WriteReadData/8431.pdf

whether it is to be treated as a Sectoral Code of Practice under the ambit of Section 50 of the PDP Bill that the DPA has the powers to further refine. Similarly, the grievance redress mechanism provided for in Para 32 of the draft Health Data Management Policy does not clarify if a data principal who is dissatisfied with grievance arbitration of the Data Protection Officer of the National Digital Health Mission can approach the DPA.

ii. Lack of institutional safeguards for processing of sensitive personal data.

The draft Health Data Management Policy mandates *ex-ante* data protection impact assessment by the data fiduciary only in instances where a risk of significant harm to data principals is perceived. However, this is much narrower in scope than Section 27(1) of the PDP Bill, which recognises the need for such impact assessment also in the processing of sensitive personal data, such as biometric and genetic data, or in any processing that may lead to profiling. It is worth noting that there exists a risk of 'significant harm' in every act of processing of sensitive personal data, including biometric and genetic data.

2.3. Lacunae from the PDP Bill that are perpetuated in this Policy

The current draft of the PDP Bill has the following lacunae that are particularly problematic for data governance in the health sector.

i. Lack of a right to explanation.

The PDP Bill has limited the 'right to explanation'[8] to a narrow right "*to access a brief summary of processing activities undertaken by the data fiduciary with respect to the personal data of the data principal.*" In the NDHE, where wide data sharing between public and private health information providers and users is envisaged, the absence of a broader right to explanation that enables access to pertinent and meaningful information about the logic involved in automated decision-making will have major repercussions for transparency and accountability in health data governance.

ii. Lack of clarity in the conceptualisation of 'health data.'

The term 'health data' has not been defined in the draft Health Data Management Policy though physical, physiological and mental health data have been acknowledged to be a part of 'sensitive personal data.' Presumably, the draft Health Data Management Policy is operating with the definition of 'health data' provided in the PDP Bill. According to Section 3(21) of the PDP Bill, 'health data' "*means the data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal,*

8 Aggarwal, N.M. & Chima, R.J.S. (2019, February 24). *India's Data Protection Bill: Further Work Needed in order to Ensure True Privacy for the Next Billion Users.* AccessNow. https://www.accessnow.org/cms/assets/uploads/2020/02/Access-Now-Analysis-Indias-Personal-Data-Protection-Bill-2019.pdf

data collected in the course of registration for, or provision of health services, data associating the data principal to the provision of specific health services." This definition is very limited in the current context of datafied health services. Health data today is not only collected in the context of clinical practice or even health services provisioning, but also from social media and other behavioural data footprints largely through inferential analytics. As the EU General Data Protection Regulation (GDPR) has acknowledged, health data is all 'data concerning health'[9] and all health data is a type of sensitive personal data (Article 9) which may only be processed under a professional or statutory obligation of secrecy.[10]

iii. Limited imaginary of 'harm.'

Health data processing without adequate safeguards could lead to both collective and individual harms. Unfortunately, the draft Health Data Management Policy limits its conception of 'harms' to those that are likely to stem from health data processing, and extending to the individual harms of *"bodily/mental injury, financial/property loss, reputational harm, loss of employment, discriminatory treatment, blackmail/extortion, denial/withdrawal of services, speech/movement restrictions and surveillance."* In this, it mirrors the narrow conceptualisation of harm outlined in the PDP Bill. As scholars have highlighted,[11] the processing of genetic and biometric data has the potential to entrench bias and group discrimination against members of religious, racial, ethnic and geographic minorities in automated decision-making systems. This needs to be addressed through specific provisions on 'collective harm.'

iv. No penalty for reversal of anonymisation.

The draft Health Data Management Policy, in Para 29.3, highlights that *"any entity which is provided access to de-identified or anonymised data shall not, knowingly or unknowingly, take any action which has the effect of re-identifying any data principal or of such data no longer remaining anonymised."* The PDP Bill has deemed anonymisation[12] to be irreversible if it meets standards of irreversibility specified by the DPA. Intentional reversal of de-identification is a punishable offence under Section 82 of the PDP Bill. However, currently there is neither a penalty nor a mechanism for penalising the reversal of anonymisation whether it is done "*knowingly or unknowingly.*"[13]

9 EU General Data Protection Regulation (Section 4 (15)), defines *"data concerning health"* as: *"personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".*

10 Processing of special categories of personal data. Intersoft Consulting. https://gdpr-info.eu/art-9-gdpr/

11 Tayor, L. (2019). *Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World* in Group Privacy New Challenges of Data Technologies; Hallinan, D. & Hert, P. *Genetic Classes and Genetic Categories: Protecting Genetic Groups Through Data Protection Law* in Group Privacy New Challenges of Data Technologies.

12 It is also worth noting here that anonymisation has been differently understood in PDP Bill, the Blueprint and the draft Health Data Management Policy.

13 Mittal, A. (2020, January 14). *Has India's Privacy Bill Considered the Dangers of Unrestricted Processing of 'Anonymised' Data*. The Wire. https://thewire.in/government/privacy-bill-anonymous-data

3. Absence of governance mechanisms to prevent privacy violations and corporate data capture

Para 29 of the draft Health Data Management Policy specifies that data fiduciaries, that is, public or private entities processing personal data in health settings, may make anonymised or de-identified data in an aggregated form (non-personal health data) available for "*health and clinical research, academic research, archiving, statistical analysis, policy formulation, the development and promotion of diagnostic solutions and such other purposes,*" in accordance with the procedure stipulated by the NHA. This provision is in sync with the vision of the National Digital Health Mission Strategy Overview (NDHM Strategy Overview)[14] to leverage the NDHE and its data pools as *"the core and common digital building blocks required for healthcare and make them accessible as digital public goods to both the public and private ecosystem."* [15]

A few critical concerns will arise if we realise this vision of the NDHE.

3.1. Lack of privacy and personal data protection safeguards in data sharing arrangements

The draft Health Data Management Policy attempts to provide for privacy and personal data protection safeguards in the 'sharing of de-identified or anonymised data by data fiduciaries,' but this ostensible safeguard falls short.

Para 29.3 states that entities provided access to de-identified/anonymised data in such data sharing arrangements "*shall not, knowingly or unknowingly, take any action which has the effect of re-identifying any data principal or of such data no longer remaining anonymised."* Technical processes and protocols for de-identification/anonymisation are to be specified by the NHA, in consultation with the Ministry of Electronics and Information Technology. However, a specific framework of the rights and obligations of data fiduciaries and entities participating in such data sharing arrangements with respect to preventing re-identification and reversal of anonymisation has not been spelled out.

Transparency about the manner and purpose for which data is to be used by the HIU (health information user) is necessary to audit if, and how, such use may pose privacy risks through possible re-identification. Furthermore, the obligations placed on health information users entering data sharing arrangements lack sufficiently robust transparency and disclosure arrangements. Para 30.4 states that *"A HIU shall, to the extent reasonable, maintain: (a) a record of all personal data that is disclosed to any other entity, including the names of such entities, the time at which such personal data was disclosed and the categories of personal data which was [sic] disclosed; and (b) a record of how such personal data is used by the HIU in a manner which enables the*

14 National Health Authority. (2020). National Digital Health Mission – Strategy Overview. https://ndhm.gov.in/assets/uploads/NDHM_Strategy_Overview.pdf
15 National Health Authority. (2020). National Digital Health Mission – Strategy Overview. (Section 2.1.1). https://ndhm.gov.in/assets/uploads/NDHM_Strategy_Overview.pdf

audit and review of any use of such personal data." The use of the words 'to the extent reasonable' instead of an 'obligation simpliciter' (unconditional obligation) is highly problematic as HIUs can easily evade accountability for improper documentation and audits of data sharing arrangements.

3.2. Risk of private capture of public data infrastructure

Another lacuna in the governance of data sharing arrangements is the absence of safeguards for preventing corporate capture and enclosure of valuable health data public goods by digital companies. The experiences of the United Kingdom[16] and Republic of Korea[17] in sharing health data public goods with Big Tech clearly indicate that in the absence of an institutional mechanism for the governance of such aggregate non-personal data resources through a 'commons governance framework' (data trusts), these arrangements are only going to facilitate the private capture of data public goods and unethical profiteering.

The NDHM Strategy Overview (Para 2.2.8) mentions that "*Front-end apps will not be allowed to download and store the PHR [Personal Health Record] of the patients and create their own repositories. These [apps] will also not be allowed to use the patient data for any advertising, commercial or profiling purposes*". Unfortunately, such use limitation does not expressly find mention in the draft Health Data Management Policy.

4. Risks of exclusions from health services

4.1. Risk of enrolment in the ID becoming mandatory by default

The claim of the draft Health Data Management Policy that joining the Health ID System is 'purely voluntary in nature' is not borne out by the policy documents governing the NDHE. While the draft Health Data Management Policy states that setting up a Health ID is *"is purely voluntary in nature, based on the consent of individuals,"* accompanying documents that are to be read with it suggest this is a facetious claim. The NDHM Strategy Overview mandates that the Ministry of Women and Child Development shall link all data with Health ID.[18] Further, the Guidelines for Health Information Providers, Health Repository Providers, Health Information Users and Health Lockers[19] provide that "*several Government schemes may accept only Aadhaar linked Health IDs."* These Guidelines for Health Information Providers and others also mandate the creation of compulsory Health IDs for

16 Molloy, C. (2020, March 3). *Will Big Tech save the NHS – or Eat It Alive?*. Open Democracy. https://www.opendemocracy.net/en/ournhs/will-big-tech-save-the-nhs-or-eat-it-alive/

17 Kim, C. (2013, December 9). 1*0,000 Korean Doctors Protest Hospital Privatization*. Korea Bang. https://www.koreabang.com/2013/stories/10000-korean-doctors-protest-hospital-privatization.html'; Kelsey, J. (2020). *Digital Trade Rules and Big Tech: Surrendering Public Good to Private Power*. Public Services International. https://publicservices.international/resources/publications/digital-trade-rules-and-big-tech-surrendering-public-good-to-private-power?lang=en&id=10825&showLogin=true

18 National Health Authority. (2020). National Digital Health Mission – Strategy Overview. (page 31, Annexure 2). https://ndhm.gov.in/assets/uploads/NDHM_Strategy_Overview.pdf

19 National Health Authority. (2020). National Digital Health Mission Guidelines for Health Information Providers, Health Repository Providers, Health Information Users and Health Lockers. https://ndhm.gov.in//assets/uploads/HIP_HIU_Policy.pdf

infants and newborn children. The meaning of voluntariness thus stands vitiated with a lack of coherence on this vital issue across related policy documents, effectively diluting the claim and pushing towards a default mandatoriness.

Experiences with Aadhaar ID show how it has become mandatory in practice, in total violation of the judgment by the Supreme Court of India[20] in the case of *K. S. Puttaswamy & Anr. vs. Union of India & Anr.*[21] Such de facto mandatoriness in the rolling out of Aadhaar IDs comes at heavy costs, resulting in exclusions and delegitimising rightful claims of those already marginalised.[22] Similar experiences, with equally devastating consequences, could follow in the event that the Health ID becomes de facto mandatory for access to essential public services like healthcare. It is concerning that the Chandigarh Administration has already issued Health ID cards, further directing local authorities to "*ensure that all employees working under them must register and get their digital cards within a week.*"[23]

4.2. Risk of children being denied health services

Similar to the PDP Bill, the draft Health Data Management Policy mandates that in the case of processing of personal/sensitive personal data pertaining to a child, data fiduciaries are obligated to obtain the consent of parents/guardians. It is important to flag that in the health care setting, adolescents who have not attained the age of majority may seek contraception or other reproductive health services without the knowledge of their parent/guardian. There is no explicit safeguard ensuring that children independently seeking health services are not denied such services because of the failure to produce parental/guardian consent for data processing. The absence of such a proviso in Para 12 pertaining to parental/guardian consent for processing personal data of children is likely to compromise their right to health.

5. Recommendations

Based on a close reading of the draft Health Data Management Policy, the Blueprint and the NDHM Strategy Overview, we would like to make the following recommendations.

5.1. PDP Bill a necessary precursor to a Health Data Management Policy

The decision to bring in place a policy on health data management without a data protection law is in contravention of the Supreme Court's decision in *K. S. Puttaswamy & Anr. vs. Union of India & Anr*.[24] However, certain aspects of the PDP Bill, currently under parliamentary review, must be

20 Bhattacharya, A. & Anand, N. (2018, September 26). *Aadhaar is Voluntary—But Millions of Indians Are Already Trapped*. Quartz India. https://qz.com/india/1351263/supreme-court-verdict-how-indias-aadhaar-id-became-mandatory/
21 *K. S. Puttaswamy & Anr. vs. Union of India & Anr.* (2019) 1 SCC 1.
22 Re-Think Aadhaar. (2018). Exclusions. https://rethinkaadhaar.in/testimonials
23 PTI. (2020, August 20). *Digital Health, One Nation One Ration Cards Launched in Chandigarh*. Mint. https://www.livemint.com/news/india/digital-health-one-nation-one-ration-cards-launched-in-chandigarh-11597940524976.html
24 *K. S. Puttaswamy & Anr. vs. Union of India & Anr.* (2019) 1 SCC 1.

revisited and amended. The personal data protection law must i) include a meaningful right to explanation; ii) expand its conception of health data to 'data concerning health,' clearly covering the context of datafied health services; iii) broaden its conception of 'harm,' especially 'significant harm,' to accommodate collective harm; iv) put in place systemic safeguards to protect privacy rights in aggregate and anonymised data.

5.2. Jurisdictional subordination of the NHA to the DPA

The draft Health Data Management Policy should expressly mention that it is a sector-specific mechanism to govern health data, as envisioned under the proposed PDP Bill, to avoid future operational confusion. The DPA should be the final authority having jurisdiction over the interpretation of provisions of the draft Health Data Management Policy. Making this explicit will avoid any future jurisdictional conflict between the NHA and the DPA.

5.3. De-facto voluntariness of the Health ID

The Health IDs conceived by the draft Health Data Management Policy must remain voluntary in the true sense of the term, remaining unlinked to the Aadhaar database, and not become mandatory by default. The Supreme Court in *K. S. Puttaswamy & Anr. vs. Union of India & Anr.*[25] categorically stated that the Centre expanding the purpose of Aadhaar beyond that permitted in the corresponding legislation would be a disproportionate intrusion into the realm of individual privacy, and therefore run afoul of the Constitution of India. Linking the Health IDs to the Aadhaar database would constitute such overreach.

5.4. A sector-specific health data protection law

A robust framework for protection of health data needs legislative protection, wherein the rights and interests of data principals can be protected and enforced. A global review of good practices indicates that the enactment of a personal data protection framework followed by sector-specific legislation on health data is the desired route for effective data governance in publicly provisioned digital health infrastructure.[26]

5.5. Institutional safeguards for processing sensitive and personal data

Ex-ante data protection impact assessments should be done for all instances of processing that carry the risk of profiling, including any processing of sensitive personal data, such as biometric and genetic data, to mirror privacy protections in the PDP Bill.

25 *Ibid.*

26 OECD has recommended that the enactment of personal data protection legislation must precede the evolution of specific frameworks for health data governance, in OECD (2019), *Health in the 21st Century: Putting Data to Work for Stronger Health Systems*, OECD Health Policy Studies, OECD Publishing, Paris, https://doi.org/10.1787/e3b23f8e-en. Experiences of Estonia (Health Services Organization Act, 2002), England (The Data Protection Act 2018) and Republic of Korea (Personal Information Protection Act, 2011 and 2004 Bioethics Safety Act) indicate that specific parliamentary legislation on digital health infrastructure, in addition to overarching personal data protection legislation, is desirable for robust personal data governance in the health sector.

The draft Health Data Management Policy's mandate of submitting a valid proof of relationship and valid proof of identity of parent/guardian to the data fiduciary to process the personal data or sensitive personal data of a child needs to be revisited. A proviso should be placed in Para 12 ensuring that children independently seeking reproductive health services are not denied access because of the mere failure to produce parental/guardian consent for data processing.

5.6. Preventing capture of public data infrastructure by private entities

The draft Health Data Management Policy must have provisions to safeguard privacy in data sharing arrangements as well as ensure that repositories of patient data records are not created by private entities for commercial purposes. This can be achieved by placing a use limitation – as spelt out in the NDHM Strategy Overview against *"any advertising, commercial or profiling purposes"* – in Para 26.6 of the draft Health Data Management Policy. These limits should be extended to data management practices laid out for data processors under Para 27.2 and to safeguards created under Para 25.2 for sharing of data linked to Health IDs.

5.7. Explainability and valid consent

Any privacy notice specification, as conceived in Para 10.4 of the draft Health Data Management Policy, should not only ensure access to information, but also the explainability of such health data related information. The burden-of-proof for acquiring valid consent should be placed directly on the data fiduciary, as the framework of the PDP Bill also envisions (Clause 11(5)).

5.8. Harmonisation of definitions across statutes

The terms 'personal data,' 'anonymisation,' and 'processing,' should be reconciled against the law that is enacted for personal data protection. The draft Health Data Management Policy should not rely on definitions from a data protection legislation that has not been enacted. It should expressly define terms like 'consent manager,' 'health data,' and 'personal data breach.' The definition of 'significant harm' should include inferred data to prevent the risk of deleterious effects on the privacy rights of groups/communities. Categories for significant harm that are especially pertinent to health data, like 'genetic data' and 'biometric data' must be defined expressly in the draft Health Data Management Policy. Unless these definitions are clear and unambiguous, transparency and accountability in the implementation of a health management law or policy will not be assured, particularly in the fraught context of health data.

5.9. Need for consultative processes

When proposing a law or policy with constitutional import, it is incumbent on the Government to provide a consultation period of a minimum of thirty days, as laid out in the Pre Legislative

Consultancy Policy, 2014.[27] In the present case, much-needed time for public consultation to encourage multi-constituency engagement on vital issues pertaining to the governance of proposed health infrastructures has been denied. Given the far-reaching implications of the proposed policy, the draft needs to go through consultations with the wider community working on the right to health and health data ethics.

5.10. Vital role of state governments in matters relating to public health

The central government must expressly seek the advice of state governments before launching a health data management policy that encroaches on the distribution of powers in the schema envisaged by the Constitution. In the existing scheme for the distribution of powers, state governments are primarily responsible for public health; yet, the central government has developed policies in this regard, although it lacks the constitutional power to do so.[28] Several state governments have had great success in implementing health-related policies such as National Rural Health Mission and the National Health Mission using Internet and communication technologies to connect public health centres in remote tribal areas. Insights from these initiatives would have ramifications on the creation of new health-related digital infrastructures and must be taken into account.[29] Introducing a policy to manage health data, which demands contextual, hyper-local responsiveness, without holding a consultative process where state governments are at least equal participants, is in abrogation of the rule of law and adversely impacts the spirit of cooperative federalism vital to our Constitution.[30]

27 Singh, R. (2020, May 5). *India Needs an Institutional Framework for Pre-Legislative Consultations*. CLPR. https://clpr.org.in/blog/india-needs-an-institutional-framework-for-pre-legislative-consultations/
28 Shah, S. & Atreya, S. (2020, June 15). *COVID-19 Outbreak Refocuses Need to Shift Public Healthfrom State to Concurrent List; Move Won't Harm Decentralisation but Enhance Centre, State Coordination.* Firstpost. https://www.firstpost.com/health/covid-19-outbreak-refocuses-need-to-shift-public-health-from-state-to-concurrent-list-move-wont-harm-decentralisation-but-enhance-centre-state-coordination-8483911.html
29 Oommen, P.J. & Antony, K.R. (2020, September 4). *Mind the gaps in India's health care digital push.* The Hindu, https://www.thehindu.com/opinion/lead/mind-the-gaps-in-indias-health-care-digital-push/article32517477.ece
30 *Ibid*.