The Lakshmi Mittal and Family
SOUTH ASIA INSTITUTE
HARVARD UNIVERSITY

RESPONSE TO

THE INVITATION FOR PUBLIC COMMENT

NATIONAL DIGITAL HEALTH BLUEPRINT

4th AUGUST, 2019

IDHN
India Digital Health Net

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The India Digital Health Net (IDHN) at the Lakshmi Mittal and Family South Asia Institute at Harvard is a research and policy collaborative focused on the development of a patient-centric, provider-friendly, Application Programming Interface (API)-enabled health exchange ecosystem. Partners in India and the United States include technical and legal experts, medical practitioners and policy makers.

In 2016, members of this group convened a conference, Reimagining Health Data Exchange: An API-enabled Road Map for India. The deliberations were captured in a paper by the same name, in the Journal of Medical Internet Research (https://www.jmir.org/2018/7/e10725/),published in July 2018. We were pleased to see the principles outlined therein, calling for a federated Personal Health Record (PHR)-enabling architecture, subsequently reflected in NITI Aayog's National Health Stack design.

In 2018, we submitted a detailed response to the Government of India-appointed Justice Srikrishna Committee of Experts on Data Protection Framework for India, discussing the implication of the proposed data protection laws on care delivery, equity, fairness and adoption of novel technologies. (https://fxb.harvard.edu/2018/02/08/harvard-fxb-responds-to-white-paper-on-data-protection-framework-for-india/)

Our members have inter-sectoral expertise in a range of domains including developing consumer or provider facing digital health technology solutions, developing system-wide health information exchanges, and formulating policies on clinical research, human rights and health data privacy. Several of us are practising clinicians.

We are very pleased to see the National Digital Health Blueprint (NDHB) – a grand undertaking, that executed correctly, can profoundly improve access and quality of care. It also lays the foundation for accelerating medical research and harnessing the power of evolving big data and machine learning technologies. However, it is now, when these prototypes are in their nascent stages, that due diligence is required to ensure that such massive technological shifts do not also cause inadvertent harm to patients or populations.

On July 16, in response to the Ministry's call for public comment, colleagues at St. John's Research Institute and IDHN reached out to experts from across disciplines, all of whom work on some aspect of developing, analysing, designing, critiquing or using digital health systems. A list of contributors follows this note.

Process

Each collaborator was invited to post comments on a shared document, accessible to the entire group. Domain experts were tagged with questions, and queries resolved publicly within the group. Daily communication through email, shared online documents, and texts were rounded off with two-group wide conference calls to reach consensus on key themes. All collaborators signed off on the final draft.

We summarise here the key themes we have addressed in the document:

Federated Architecture

We believe that the NDHB needs to further elaborate its vision for the federated architecture. There are sections of the NDHB that advocate for Central Repositories and exports of data to the PHR whenever new data are generated. Other sections mention collation of only metadata via reference links. We believe this latter model, as was also proposed by the National Health Stack via the Health Data Fiduciaries, is the superior one.

The NDHB outlines a vision where much of the development is centralised, and the role of state agencies, the non-government sector, the private sector and the open source communities are not articulated. We strongly advocate for a larger role for open source development. After all, clinical medicine is an open source practice, teachable and modifiable at the local level by licensed practitioners.

Patient Safety

We urge that the NDHB address patient safety more expansively. This large technological enterprise (combined with rapid advances in machine learning and Artificial Intelligence (AI)) expose the patient to several risks - including denial or delay of services, being subject to non-transparent decision support tools, black-box algorithms, and so on - all of which are real, and supported by an evolving body of literature. It is imperative that transparency and auditability be embraced as non-negotiable, across this system.

Privacy Protection

We discuss at some length the need to combine Consent, Anonymisation (and other data protection measures) and a Fiduciary Responsibility on Data Controllers, to protect privacy and security. Over reliance on anonymisation will fail in the face of evolving AI technologies. We also recommend that anonymisation happens as close to source as possible, and is not a centralised and distal function, as currently ascribed to the Anonymiser.

Grievance Redressal

The NDHB does not address Grievance Redressal. We advocate for Grievance Redressal to be considered an important building block and one that provides timely feedback to the design process, especially at these initial stages, where reported grievances are likely to be signals for system-wide limitations or failures.

Change Management

We wish to underscore the importance of Change Management and urge that the next iteration of this document outline in rich detail its theory of change, with emphasis on training, support, re-training, and upgrading skills sets, across the system. We also note that the reliance on smartphones and Mobile First sentiment may be premature. Recent studies estimate smart phone penetration at about 24%.

Optimisation Vertical

Many of the components of the proposed architecture have not been tried in India, and never at such scale anywhere in the world. We recommend the creation of a Prototyping Building Block, linked closely to a Regulatory Sandbox, that allows for testing and rapid iterations of all critical components of the design. This prototyping environment will allow the rapid and simultaneous testing of alternate models; provide interoperability testing labs; and continuously solicit feedback and respond to the system. We believe this cycle of testing, feedback (including grievance redressal), and rapid prototyping constitute a third vertical - an Optimisation Vertical, critical to the success of the NDHB.

As transactional as the arrangements between these various blocks and layers may seem to be, we must recognise that human health is not a commodity, and all components of the proposed architecture must enhance (and not imperil) access to care and quality of care, even for the millions that are not yet members of the digital grid.

Finally, we wish to thank two colleagues in particular, Nivedita Saksena, of the Harvard TH Chan School of Public Health, and Jimmy Antony, from the St. John's Research Institute for their tenacious commitment to organising, writing and editing this document.

We commend the bold vision laid out in the NDHB. Executed thoughtfully, and along realistic timelines, it can profoundly enrich the healthcare experience for over a billion people.

Sincerely,

On behalf of our co-respondents,

Dr. Satchit Balsari, MD, MPH
Assistant Professor, Emergency Medicine,
Harvard Medical School/Beth Israel Deaconess Medical Center.
Harvard FXB Centre for Health & Human Rights.
Burke Fellow, Harvard Global Health Institute.

Dr. Tony D S Raj, MBBS, MD
Dean,
Head, Division of Medical Informatics
St. John's Research Institute.

LIST OF RESPONDENTS

Abhijit Gupta: Co-Founder and CEO, Praxify Technologies

Abijeet Waghmare: Manager, Medical Informatics & Innovations, St. John’s Research Institute

Adrian Gropper: Chief Technology Officer, Patient Privacy Rights

Angshuman Sarkar: Principal Consultant, ThoughtWorks

A V Sethuraman- Senior Vice President, Argusoft

Devesh Varma: Vice President & Chief Technology Officer, Piramal Swasthya

Dhruv Pandey: Portfolio Manager at Social Alpha (Tata Trust)

Harpreet Singh: Scientist and Head, Informatics, Systems & Research Management, Indian Council of Medical Research, Government of India

Jimmy Antony: Medical Informatics Consultant, St. John’s Research Institute

John Halamka: International Healthcare Innovation Professor of Emergency Medicine, Harvard Medical School; Director, Health Technology Exploration Center, Beth Israel Lahey Health

Namrata Arora: Senior Consultant, India Digital Health Net

Nivedita Saksena: Harvard University

Rahul Matthan: Partner, Trilegal

Satchit Balsari: Assistant Professor, Emergency Medicine, Beth Israel Deaconess Medical Center & Harvard Medical School; Harvard FXB Centre for Health & Human Rights; Burkle Fellow, Harvard Global Health Institute

Sneha Vaidhyam: Research Associate, St. John’s Research Institute

Sunita Nadhamuni: Head, Healthcare Solutions, DellEMC

Supten Sarbadhikari: Independent Consultant for Digital Health

Tarun Khanna: Jorge Paulo Lemann Professor, Harvard Business School; Director, Lakshmi Mittal and Family South Asia Institute, Harvard University

Tony Raj: Dean, St. John's Research Institute; Professor of Physiology, St. John’s Medical College; Head, Division of Medical Informatics, St. John’s Research Institute

Vivek Divan: Independent Consultant - Health, Sexuality, Law, Human Rights

ABOUT THIS DOCUMENT

All chapter numbers, headings, and paragraph numbering correspond to their respective counterparts in the original National Digital Health Blueprint released by the Ministry of Health and Family Welfare, Government of India, and accessible at: https://mohfw.gov.in/sites/default/files/National_Digital_Health_Blueprint_Report_comments_invited.pdf (accessed August 4, 2019)

CHAPTER 1: SCOPE AND CONTEXT

1.1. The Context

Key Issues: 1) There has been an exponential rise in mobile and digital health interventions in India in recent years, with significant public sector resources dedicated to digitising public health data, often at source. Bassi et al., in a review of 300 articles in 2018, underscored the urgent need for focused research aimed at generating high-quality evidence on the efficacy, user acceptability, and cost-effectiveness of mHealth interventions aimed toward health systems strengthening.[1] It is recommended to include an implementation research component into the existing and proposed digital health initiatives to support the generation of evidence for health systems strengthening on strategically important outcomes. Furthermore, there is a need for greater evidence that the vast amounts of data so digitised have been analysed and acted upon to benefit the communities the data are generated in.

Recommendation:

1. It may be advisable to create Regulatory Sandboxes in various jurisdictions across India, to rapidly test prototypes that are being proposed by the National Digital Health Blueprint (NDHB), before they are adopted at national scale. Such an approach will allow solutions to have contextual intelligence and may reveal the need to permit greater flexibility and variability in the proposed model to account for the wide social, cultural and economic diversity in India's population.

Regulatory Sandboxes must be accompanied by clear boundary conditions, data governance measures and risk mitigation strategies, as has been instituted, for example, in Singapore for telemedicine initiatives.[2] Guidance may also be sought from the proposal of the Reserve Bank of India for regulatory sandboxes in the fintech space. In Chapter 5, we elaborate how learnings from these Regulatory Sandboxes can provide feedback to the system, through an "Optimisation Vertical" we have proposed.

1.2 Vision of the National Digital Health Blueprint

Key Issues: 1) Given the rapidly growing number of novel data streams (from mobile phones and other wearables), it would be important for the NDHB to define "health data" or articulate a policy that recognises that the definition may need to evolve. For example, researchers use data from the gyroscope and accelerometer in mobile phones to monitor tremors, or track mobility to predict depression. It is not unreasonable to imagine that such data points may eventually be considered valid and routine diagnostic adjuncts. Recognising these uses of data, the General

[1] Bassi A, John O, Praveen D, Maulik PK, Panda R, Jha V. Current Status and Future Directions of mHealth Interventions for Health System Strengthening in India: Systematic Review. JMIR Mhealth Uhealth [Internet]. October 2018; Vol. 6 (10). Available from https://mhealth.jmir.org/2018/10/e11440/.

[2] Ministry of Health Singapore [Website]. Licensing experimentation and adaptation programme (LEAP)- a MOH regulatory sandbox. Available on: https://www.moh.gov.sg/our-healthcare-system/licensing-experimentation-and-adaptation-programme-(leap)---a-moh-regulatory-sandbox

Data Protection Regulation (GDPR) defines any data which reveals information about the health status of an individual as health data.

Recommendations:

1. The NDHB must define Health Data, such that it allows for novel new data sources to be included and aligns with key domestic laws especially the Personal Data Protection (PDP) Bill.

1.3 Objectives of the National Digital Health Blueprint (NDHB)

Key Issues: 1) The objectives listed in the NDHB are very comprehensive. While they address the need to enforce adoption of standards by all actors in the ecosystem, we recommend further clarity on adoption drivers for the private sector, a large and growing player in the healthcare delivery system now envisioned for India. The NDHB references NITI Aayog's Strategy and Approach document for the National Health Stack (NHS), released in July 2018. The NHS required that private providers would be an essential stakeholder in a federated architecture for effective service delivery, quality and continuity of care. This would require them to be compliant with NHS information exchange protocol and policies in order to ensure "continuity of care," - a key component of Pradhan Mantri Jan Arogya Yojana (PMJAY) as well. This principle of continuity of care undergirds the need for a personal health record as well. Such enforcement in the private sector may be ensured by mandate or incentive. But implementation may be challenging without robust enforcement ability. For instance, a mandate for private providers to notify tuberculosis cases to the Nikshay system has seen a lukewarm response from practitioners as they have seen it as a potential revenue loss once the TB patient was notified and referred to a public facility. Private sector buy-in may require combining a rigorous campaign of awareness and patient-driven demand, with mandates and incentives. Given that the majority of health service delivery occurs at the primary care level (whether in the urban or rural setting), subsequent versions of this document should ideally address drivers for user adoption in this large group of providers. While PMJAY may be a catalyst for driving adoption, relying solely on PMJAY may not work: In the state of Karnataka, for example, there are only 776 empanelled facilities, and most healthcare interactions will occur outside the purview of PMJAY. The solo general practitioners providing primary care are also currently beyond the scope of PMJAY.

While a fraction of the private sector may indeed be incentivised to digitise, by making it a prerequisite to participate in PMJAY schemes, it is this very insurance sector driven adoption of digital health records that may preclude widespread acceptance, if clinicians and patients perceive little direct value from it. Placing clinical and public health needs front and center will drive adoption by increasing demand.

2) We also introduce the concept of substitutability here as an additional but key goal of the NDHB. Mandl et al explain, "The system should be sufficiently modular and interoperable so that a primary care provider could readily use a billing system from one vendor, a prescription-writing program from another, and a laboratory information system from yet another. Individual systems

do not need to perform all functions."[3] This guiding principle will prevent monopolies and foster competition, allowing market forces to optimise the user experience of health technology. Monolithic and monopolistic Electronic Health Records (EHR) in the United States have contributed to alarming physician burnout - a scenario India can hardly afford to replicate. Balsari et al. have also underscored the importance of substitutability as a critical element of successful health information ecosystems.[4]

3) We observe that the articulated vision of "ensuring the security, confidentiality and privacy of health-related personal information" (ab-initio, by design) does not manifest in the listed goals. Transparency would be key to the platform's acceptability and success. The ability to trace and audit use would be critical to maintaining trust in the system. Emerging technologies such as blockchain could be leveraged to build trust across multiple levels in the platform. Blockchain can help verify physician identity and licensing; ensure immutability at source of data collected as a part of care, and enhance informed consent frameworks. These measures that engender trust should find inclusion in the NDHB and be bolstered by scientific evaluation of the efficiency of blockchain technology.[5],[6]

4) We have discussed the implications of using Clinical Decision Support (CDS) systems in light of patient safety, quality of care, and fairness, in subsequent sections.

Recommendations:

1. Articulate the terms of engagement with the private sector.
2. Substitutability is an important operational goal that must be included in this list.
3. The NDHB must explicitly also include the protection of patient privacy, security of health data, continuity of care and transparency of functioning in its stated objectives.
4. Describe the timelines, incentives, budgets, maintenance plans for directories and registries
5. Quality and performance metrics must be formulated after consultations with professional societies and patient advocacy groups.

[3] Mandl K, Kohane I. No Small Change for the Health Information Economy. New England Journal of Medicine [Internet]. Mar 26, 2009. Available from https://www.nejm.org/doi/full/10.1056/nejmp0900411.

[4] Balsari S, Fortenko A, Blaya JA, Gropper A, Jayaram M, Matthan R, Sahasranam R, Shankar M, Sarbadhikari SN, Bierer BE, Mandl KD, Mehendale S, Khanna T. Reimagining Health Data Exchange: An Application Programming Interface–Enabled Roadmap for India. Journal of Medical Internet Research [Internet]. Vol 20, No 7 (2018): July. Available from https://www.jmir.org/2018/7/e10725/

[5] Donovan F. BIDMC CIO lays out 3 good use cases for healthcare blockchain. HIT Infrastructure [Internet]. 2019 Feb 25. Available from https://hitinfrastructure.com/news/bidmc-cio-lays-out-3-good-use-cases-for-healthcare-blockchain

[6] Cohen J. 4 thoughts on blockchain from Beth Israel Deaconess CIO Dr. John Halamka. Becker's Healthcare [Internet]. 2019 April 6. Available from https://www.beckershospitalreview.com/healthcare-information-technology/4-thoughts-on-blockchain-from-beth-israel-deaconess-cio-dr-john-halamka.html

1.4 Overview of the National Digital Health Blueprint

Recommendation:

1. The notion of Core and Reusable Applications and Services as part of the Application Layer may be further strengthened by maintaining them as Free and Open Source Software (FOSS), supported by an active open source community.

1.5 Core Principles of National Digital Health Blueprint

Key Issues: 1) Identification: We recommend the use of Good ID Principles[7]; we have discussed the PHI in some detail in subsequent sections.

2) Trustworthiness: We address transparency and accountability in the system, and the notion that consent, fiduciary obligation and anonymisation (and other such privacy protection tools) should be combined to ensure secure, safe and authorised dataflows.

3) Longitudinal Health Record: It is important to have not only an incremental record of health events recorded in the personal health record, as it is to have a record that is portable, complete and controlled by the patient - attributes that are supported by the NDHB.

4) Consent Management: Consent has been discussed at length, but we draw your attention to the need to articulate the relationship between Consent and privacy and confidentiality. Consent, whether informed, uninformed, or waived, does not absolve data controllers from their fiduciary obligations to maintain security and privacy. Do consent artefacts that are being proposed, like the Ministry of Electronics & Information Technology (MeitY) digital consent artefact, allow the system to flag violations?

Table 1.1 : Business Principles

NDHB will be wellness-centric and wellness-driven

Key Issue: 1) The data protection law requires data minimisation, which is desirable. Yet, forcing minimisation may impede the wide-ranging future possibilities offered by Artificial Intelligence (AI) and Machine Learning (ML) to influence health, habits and lifestyles.

NDHB shall educate and empower citizens to avail a wide range of health and wellness services

Key Issue: 1) The NDHB does not adequately address the role of civil society, patient groups, and professional societies in helping formulate National Digital Health Mission (NDHM) policies that can have far reaching impact on their lives and wellbeing.

[7] Digital Identities: Design and Uses [Website]. Towards a framework for evaluation of digital ID. 2019 June 11. Available from https://digitalid.design/evaluation-framework-01.html

Recommendations:

1. The NDHB should describe how digital awareness will be promoted across society and across all key players, to help all participants recognise the value of digitisation, the limitations of digital data, the vast potential and limits of the digital ecosystem and the scale, limitations and biases associated with automated decision tools.
2. The NDHM vision will also require managing change; educating, training (and re-training), and supporting a large cadre of health sector professionals in the design, development and use of digital tools.

NDHB systems shall be designed to be inclusive.

Recommendation:

1. The scope of inclusivity here must account for biases inherent in health data and health delivery systems that go beyond terrain limitations. Moreover, initiatives like telemedicine should not be considered stand-alone technological solutions to delivery problems, but one adjunct to task-shifting and supervision, to improve care in remote regions.

NDHB shall ensure security and privacy by design

Key Issue: 1) The National Digital Health Ecosystem (NDHE) will be governed by the Personal Health Data Protection bill, when passed into law. What we anticipate will be challenging is the existence of several overlapping health sector specific laws that have evolved over time, and that determine various aspects of consent, privacy and data flow, ranging from the Mental Healthcare Act, 2017, to the HIV/AIDS Act, 2017 and the Transplantation of Human Organs and Tissues Act, 1994.

Stronger lateral linkages must also be established with other policies/guidelines such as National Data Sharing and Accessibility Policy (NDSAP), Department of Biotechnology’s Biological data storage, sharing and access Policy and many institutional policies.

Recommendation:

1. The transparency and accountability necessary to make NDHM a success is best supported by an accompanying regulatory framework that allows enforceability. Fast evolving machine learning and AI technologies are challenging long accepted notions of how data may be secured. A code of practice in line with the Data Protection Bill that speaks to these challenges while dealing with health data, is warranted.

NDHB shall be designed to measure performance and display accountability of all providers of service.

Key Issue: 1) How quality of care is measured in the Indian context is yet to be determined. That quality needs to be better measured is a given, but what data will be collected, what metrics will be measured and how reliably these data will represent true care delivery needs to be examined.

Existing models elsewhere, including in the US, are far from ideal. The Medicare Access and CHIP Reauthorization Act (MACRA)combines parts of the Physician Quality Reporting System (PQRS), Value-based Payment Modifier (VBM), and the Medicare Electronic Health Record (EHR) incentive program into one single program called the Merit-based Incentive Payment System, or "MIPS." Using a composite performance score, eligible professionals (EPs) may receive a payment bonus, a payment penalty, or no payment adjustment, based on quality, resource use, clinical practice improvement activities, and meaningful use of certified EHR technology. This approach while well-intentioned has led to significant gaming of the system and directly contributed to physician burnout [8,9,10,11,12]

And yet, there is ample evidence in India where the quality of care is well below par, that technological and digital adjuncts are desperately needed to promote task-shifting, support providers, monitor compliance, provide decision support, and scale training.

Recommendations:

1. Wider consultations with patient groups, practitioners, and professional societies will help determine appropriate and effective performance metrics.
2. Apply design thinking principles while developing data capture mechanisms to measure performance without reverting to provider-initiated electronic forms as the default.

Table 1.1 : Technological Principles

All the building blocks and components of the NDHB shall conform to open standards, be interoperable and based on Open Source Software products and open source development:

Key Issues: 1) This Principle is important: Standards take time to roll out across the ecosystem and are subject to "regulatory capture" - a prominent problem in the US system. By mandating open source standards, adoption does not become a competitive risk because vendor lock-in is impractical. This also accelerates standards development. Open source and standards complement one another and should both be mandated. (Of note: open standards (without the

[8] Nabhan C, Jeune-Smith Y, Klinefelter P, Kelly R, Feinberg B. Challenges, Perceptions, and Readiness of Oncology Clinicians for the MACRA Quality Payment Program. JAMA Oncology [Internet]. 4(2), 252–253. DOI: https://doi.org/10.1001/jamaoncol.2017.3773

[9] McWilliams JM. MACRA: big fix or big problem? Annals of Internal Medicine [Internet]. 2017;167(2):122–124. DOI: https://doi.org/10.7326/M17-0230

[10] Lindstorm R. Regulatory burdens contribute to physician occupational burnout. Healio Ocular Surgery News [Internet]. 2016 February 10. Available from https://www.healio.com/ophthalmology/regulatory-legislative/news/print/ocular-surgery-news/%7Bd29e74c1-0ee8-4d8b-9a70-2b943620c54b%7D/regulatory-burdens-contribute-to-physician-occupational-burnout

[11] Luh J. MACRA: regulatory burdens and the threat of physician burnout. May Clinic Proceedings [Internet]. Volume 91, Issue 11, 1671 - 1672. DOI: https://doi.org/10.1016/j.mayocp.2016.09.007

[12] Price, G. MACRA's cure may be worse than the disease. Forbes [Internet]. 2017 May 30. Available from https://www.forbes.com/sites/physiciansfoundation/2017/05/30/macras-cure-may-be-worse-than-the-disease/#4a5d9e1f474f

source) are also important because purchased standards are inaccessible to community open source projects.)

2) Many of India's societal platforms have also been built on open source software and technologies. However, the code on which these government platforms have been built are rarely if ever published. This has resulted in some form of regulatory capture or in preferential treatment being given to select players who are allowed deeper integration with the platform. This scenario may be averted by creating a public FOSS style organisation responsible for maintaining the standards and the code base for the core platform.

Recommendations:

1. An "open community" sustenance model where the state government is a significant stakeholder, but the product governance and management is done by a community process, is likely to be more sustainable and successful. An effective open source solution must be governed, managed and maintained by a dedicated community. The NDHB must articulate how the NDHM will seed and foster such communities across India.
2. However, if the applications developed in the Application layer are expected to be open source, with the attendant publication of the source code, adequate mitigation strategies will be essential to avert potential security threats. Publishing the source code as open source also ensures significant peer review and scrutiny from the wider ecosystem thus making it stronger and less vulnerable. Security standards have to be published to ensure that applications are hardened to mitigate the risk of exposing source code.
3. It is our submission that the NDHE should also make provision to accommodate applications that are not open source in the Application Layer as long as the open standards and OpenAPI requirements are met and that interoperability is ensured. This will also spur innovation from private providers in this space. [Please, however, note our concern, stated elsewhere in this document, about black-box medicine and non-transparent automated algorithms that risk turning clinical medicine -- until now an open source practice - into a proprietary transaction].
4. Consider making the platform level modules open source as well to invite wider participation and use.

Federated architecture shall be adopted in all aspects of NDHB

Key Issue: 1) The NDHB falls short of describing what the federated architecture looks like. We discuss the PHI, Personal Health Record (PHR), Health Information Exchange (HIE) and Health Locker building blocks in detail in subsequent sections.

All major legacy systems shall be assessed for conformance to NDHB principles and leveraged to the extent feasible

Key Issues: 1) The NDHB must better describe how these legacy systems, of which there are many in India, with data likely covering billions of patient encounters, are to be leveraged. The most important component of these systems is often the “data” and not the platforms per se, and matching and integrating these data across systems and to the new NDHE is likely to require significant resources. There are examples of efforts in merging legacy systems in India that have not succeeded as hoped (prime ex land records). Getting legacy systems to conform to the NDHB would likely require the implementation of an Enterprise Master Patient Index (EMPI), and the massive undertaking of matching records across systems to maintain continuity. There are no readily available or comprehensive records of database architectures across the many vertical digital repositories or precise estimates of either the quantity or quality (validity) of many of these data, making prioritisation difficult.

2) The NDHB has been prepared by a committee commissioned by the Ministry of Health and Family Welfare (MoHFW). However, other departments, like the Ministry of Women and Child Development (MoWCD) also play a significant role in care delivery - in this case, for nutrition. May we request clarification on how inputs will be integrated from across related agencies, especially in light of legacy database integration?

Recommendation:

1. Examining the true need to merge data across these systems (while being compliant with data minimisation principles mandated by local laws), and examining how (and whether) these data have been or are being used for policy making may help set priorities. After all data will be matched via Application Programming Interfaces (API) or manually (less likely) and a cost analysis to see whether the benefits of pre-loading data into new systems outweigh the costs.[13]

All registries and other master databases of NDHB shall be built as a Single Source of Truth on different aspects and backed by strong data governance

Key Issue: 1) We submit here that health data be examined in light of the PDP Bill, not as one subject to the concept of ownership, but subject to control and access. We address these concepts in the following chapters.

[13] Keshavjee K, Bosomworth J, Copen J, Lai, J, Kucukyazici, B, Lilani, R, M Holbrook, A. Best Practices in EMR Implementation: A Systematic Review. AMIA Symposium; American Medical Informatics Association [Internet]. 2006, 982. Available from https://www.researchgate.net/profile/John_Bosomworth/publication/6563679_Best_Practices_in_EMR_Implementation_A_Systematic_Review/links/02e7e5165fa6f5dd0e000000/Best-Practices-in-EMR-Implementation-A-Systematic-Review.pdf

CHAPTER 2: IDENTIFICATION & DEFINITION OF BUILDING BLOCKS

2.1 Introduction / Key Actors

Key Issues: 1) Digital services, apps, and devices should be considered integral elements of the digital health ecosystem. If harnessed well, newer digital technology-based services have shown potential to support health systems with poor capacity, for instance, provision of mental health services in low-resource settings.[14]

2) Newer categories of data will yield novel insights from connections that were previously not possible. For instance, data generated via the routine use of personal devices, wearables and social media can help generate digital health phenotypes to enhance mental health.[15] Mobile phones are being used to capture tremors in patients likely to develop Parkinson's disease before the tremors are clinically obvious. Such novel uses of, and integration of, personal devices and wearables in inevitable. The architecture must therefore have evolutionary capability (as also its accompanying regulations), guaranteeing incremental non-breaking change along multiple dimensions.

Recommendations:

1. Regulated (and unregulated) medical devices, wearables apps and digital services could be considered a separate category from pharmaceuticals.
2. The digital health ecosystem infrastructure itself (with its hardware and software components) is a distinct but central player and should be accorded greater weightage in planning and implementation.
3. Given the high proportion of out-of-pocket payments, an additional category of Payer should recognise this form of payment towards healthcare, in addition to the three identified.

2.2 Identifying the Building Blocks

Key Issue: 1) The centrality of the Personal Health Identifier to the success of the proposed system, and the importance of the Personal Health Record as a key goal for this entire exercise elevates the clinical and public health needs of patients and populations above all else and must be protected. Such a framework will help re-imagine user interfaces and digital data collection (currently the bane of EHRs in the United States) to focus on the needs of patients and providers.

[14] Naslund JA, Aschbrenner KA, Araya R, Marsch LA, Unutzer J, Patel V, Bartels SJ. Digital technology for treating and preventing mental disorders in low-income and middle-income countries: a narrative review of the literature. Lancet Psychiatry 2017 Jun;4(6):486-500. DOI: https://doi.org/10.1016/S2215-0366(17)30096-2

[15] Onnela JP, Rauch SL. Harnessing smartphone-based digital phenotyping to enhance behavioural and mental health. Neuropsychopharmacology 2016 Jun;41(7):1691-6. DOI: https://doi.org/10.1038/npp.2016.7

2.3.i : Layer 1: Infrastructure

Key Issue: 1) The NDHB recommends the government community cloud (H-Cloud) for building blocks in Layers 2 and 3 and a hybrid environment for other layers. This architecture must be revisited in the light of data localisation requirements articulated in the Personal Data Protection Bill currently in Parliament. Localisation of critical personal data while allowing mirroring or free transfer of non-critical data to hybrid entities may be desirable, to allow domestic and international cloud storage, as would be necessitated to avail of the global ecosystem of digital health services (apps, wearables, etc.)

2.3.i : Secure Health Networks

Key Issue: 1) Multiprotocol Label Switching (MPLS) or Virtual Private Network (VPN) connectivity has been recommended to secure health networks. While MPLS itself would not provide encryption, being a virtual private network, it can be partitioned off from the public internet; helps in avoiding lookups across public networks; eliminates the need for multiple layer-2 networks to satisfy different types of traffic; and speeds traffic flow. MPLS and VPN are not considered state of the art for the purposes described in the NDHB.

Recommendation:

1. Consider using Minimum Lower Layer Protocol (MLLP) for legacy Health Level Seven (HL7) v.2 transactions and RESTful architecture. [Representational State Transfer (REST) is a software architectural style that defines a set of constraints to be used for creating Web services. Web services that conform to the REST architectural style, called *RESTful* Web services (RWS), provide interoperability between computer systems on the Internet.]

2.3.i : Security and Privacy Operations Centre

Key Issues: 1) The Security Operations Centre (SOC) and Privacy Operations Centre (POC) centralises the lion's share of responsibility to secure, monitor and act on privacy and consent breaches. It is necessary to articulate here the state's capacity to manage, maintain and update such operations.

2) The Operations Centre must go beyond the traditional means of intrusion detection to monitor and respond to breaches and attacks. Leveraging Machine Learning and AI, the Centre (or a federated network of centres) must continuously analyse consent, access and usage history to proactively defend the network.

3) The envisioned architecture, perhaps aided by emerging technologies like blockchain, should facilitate contemporaneous notice of health data use to citizens similar to the notice provided for financial transactions. Access to this audit trail of data access (who, when and why) should also be available to citizens.

4) It is less clear as to how the POC will interact with the data controller under the Data Protection laws. There appears to be overlapping subject-matter jurisdiction with respect to data protection and privacy. Key questions include: Will the POC then be set up as an independent and neutral entity? What powers will it have in case data breaches/privacy violations are detected? At what levels will these audits operate?

5) Nevertheless, the concept of a sector specific privacy regulator for healthcare is useful to ensure that the nuances required in the context of health are appropriately harmonised with the broad principles of privacy set out under the Personal Data Protection Bill.

Recommendations:

1. Describe how the state will administer or delegate this substantial undertaking
2. Construct a proactive (and not merely responsive) role for monitoring security, privacy, consent and use, to predict and prevent breaches.
3. Consider making all access notifiable, as is the case with financial transactions (users may choose notification preferences)
4. Guarantee citizen access to the audit trail of data access.
5. The composition, powers and functions of the POC need clarity.
6. The POC will need to fold into the framework of the proposed PDP Bill to avoid having multiple different and mutually inconsistent standards of privacy developing in different sectors. Specifically, how the POC will interact with the Data Controller under the PDP Bill, will need to be articulated.

2.3.ii : Layer 2: Data Hubs

2.3.ii.(a) : Personal Health Identifier (PHI)

Key Issues: 1) The section “Approach to PHI” notes that the PHI system can opt for one of the three archetypes – centralised, federated and decentralised. It is recommended that the centralised approach is adopted for the following benefits: a) It is easier for a single organisation to provide and manage identifiers across the country maintaining uniqueness; b) When supported with adequate institutional mechanisms and checks, it evokes higher trust and authenticity. In this case, it is important to recognise that consent will also have to adopt a centralised approach since a divergent approach from the PHI system would be impractical.

2) However, we believe that this precludes the patient from opting to have more than one identifier, and to delink certain aspects of care data from the larger record. This is an inviolable component of healthcare delivery (and influences health seeking behaviour), and cannot be compromised. Patient MUST have the ability to NOT link a particular record (for example, a visit to an STD clinic for treatment of sexually transmitted disease) to his/her PHR, which is otherwise accessed by a wide network of their care providers. We acknowledge that there may be other mechanisms provided for records or parts of records to be delinked, without the need to create multiple IDs.

3) Conversely, maintaining a cross index of multiple identifiers in the country to accurately identify a patient is no small task and will be performance-intensive to cater to 1.35 billion. It will be equally challenging to detect and resolve duplication.

4) The Health Data Access Fiduciary (HDAF) model proposed by the NHS, and a critical component of its architecture, finds no mention in the NDHB. The HDAF model may allow for the creation of unique virtual ID across several HDAFs, does not require an EMPI, and can facilitate reference indexes to other national identifiers. Aadhar would only then be a means of authenticating the patient, without being a prerequisite for linkage or service.
Finally, it would be important to address delay of service when identification or authentication fails.

Recommendations:

1. The architecture must also allow multiple linkable IDs. Aadhar would best serve the purpose of authentication. It must further be clarified here that Aadhaar authentication can, as dictated by current law, be used only for welfare schemes notified under section 7 of the Aadhaar Act, and not generally for the provision of healthcare services. Even within this sub-group, allowing multiple identifiers is necessary given the non-negligible rates of authentication failures under Aadhaar.
2. The linkage of a visit or healthcare event to the PHI must be voluntary, and under patient control. Patients must be allowed to seek some services anonymously, with exceptions being governed by policy or law (say, for example, for notifiable diseases). Even in the case of notifiable diseases, a successfully treated Tuberculosis status or current HIV status may not be relevant to every other action in the healthcare system.
3. We recommend the use of Good ID Principles to design the digital ID.[16] This includes legislative backing for its creation, clearly specified actors and purposes, adequate redressal and accountability mechanisms and the avoidance of mission creep.
4. Articulate the NDHM policy about service denial or delays when authentication or identification fails (while needing to build in fraud protection).

2.3.ii.(b) : Personal Health Record

Key Issues: 1) The NDHB while articulating that the patient is in control of the PHR, states that the PHR generates and aggregates data. This needs additional clarity. The current wording suggests an up-to-date consolidated record, with the patient being able to consent to sharing of data from this record. This section further mentions that every time a record is created it is exported to the PHR. In that case, the data need to be stored in Secure Health Data Repositories (HDR) maintained by the government. While this model has the benefit of Data Integrity assertion (since once generated and issued, the health document is immutable), there is little evidence

[16] Digital Identities: Design and Uses [Website]. Towards a framework for evaluation of digital ID. 2019 June 11. Available from https://digitalid.design/evaluation-framework-01.html

that civil society will accept the government’s role here as the trustee of their health data (collected also from all non-public service nodes in the ecosystem).

As Professor Zuboff famously said in her book, The Age of Surveillance Capitalism, “Who decides? Who decides who decides?”

2) It would be advisable instead that the data remains at point of generation and be linked to the PHR, unless storage at point of generation is unreliable. We also believe that replicating and exporting data every time it is created is near impossible - think about streams of continuous data from a monitor, or genomic data.

3) The HDAF model proposed by the NHS describes a more passive model, with more patient autonomy. The patient could decide what to add to the PHR, could use multiple HDAFs to organise her personal records as she sees fit- aggregating some information under one HDAF and other information under another.

4) The NDHB states that the content in the PHR will need to allow for evolution, from basic content with very little metadata to a strongly structured content that meets the standards specified in Chapter 3. We submit that this design is unsafe, duplicative, undesirable and expensive. We disagree with this approach and subscribe instead to the reference indexing that the Blueprint outlines in subsequent sections in Layer 3.

5) In Layer 3, the Blueprint suggests using a reference link, where data will sit at source, but a reference link to the data will be exported to the Health Locker. This arrangement is far more desirable, provided the linking to the Health Locker is consented. Again, the HDAF architecture proposed by the NHS lends itself readily to such reference linking, blinded at both ends - the query generator and the data provider does not know the identity of the other.

6) The Blueprint mentions that the PHR shall capture the data relating to ONLY the significant medical and health episodes and events of types to be identified and notified. We believe that this needs further clarification, and while PHRs may be required to have a minimum set of data categories (whether or not the patients opt to not link to them), like a current list of medications, diagnoses, and allergies, PHRs should be allowed to have additional categories. This is where the market can play an important role and provide competitive PHR-based services and third-party applications, depending on the ability of PHRs to link with non-traditional data streams - by consent and choice.

7) We do not believe that the design of the PHR can address issues like data overload, ‘physician fatigue’, and the risk of important clinical data getting buried under other types of data. These are all a result of traditional EHRs being designed to collect medico-legal and billing information, avoiding which will depend on early attention to human-centred design in the data generation process. Most public and private sector health data applications in India are volume-heavy, and collect vast amounts of data (of questionable validity) that are seldom analysed, and almost never in a time-sensitive manner to impact real-time policy making. To address issues like data overload

and physician fatigue, data minimisation at source is key. But this requires a re-imagination of how data for payments, fraud detection, quality control and operations are collected, without providers serving as data-entry operators. Adoption of existing EHR schemas from other nations, or simple conversion of paper-based charts to radio-button infested digital forms will not work. Neither will the mere restriction of PHR metadata.

Practitioners will find PHRs useful if the data they need most (usually a *current* list of diagnoses, medications, allergies and recent events), are accessible in user-friendly, meaningful visual representations - laboratory test result trends via line graphs, for example.

8) We agree with the subsequent statements that the design of the Health Locker system, which has multiple issuers and users who can exchange data with consent and strong non-repudiation methods, should be adopted with appropriate modifications and enhancements for implementing the PHR, with the caveat that reference indices, and not data *per se* are stored in this Health Locker, were it to serve one possible PHR.

9) We note here that given the ground reality of internet and telecommunication connectivity in India, a PHR predicated on an "always on" model will be insufficient and certain critical data, and not merely reference links, should be accessible to the patient at all times - perhaps on their personal devices, with paper-based options or chip-based health-cards as a redundancy for the large swathes of the population currently without smartphones.

10) PHRs have taken multiple forms around the world. As Halamka et al explain, early PHRs were either vendor control and clinic hosted; or self-built and hospital hosted; or self-built institution-neutral hosted service, where individuals could decide who can read, write, or modify components of their records.[17] How complete the list of all problems, medications, and diagnoses must be in a PHR for it to be truly useful (or relevant), will require further consensus from the medical community in India. The authors further explain that patients may want to integrate knowledge sources and decision support systems with their PHR, participate in support communities linked by common characteristics in the PHR or participate in clinical trials, post market pharmaceutical vigilance, or public health surveillance via their PHRs.

Recommendations:

1. The HDAF model separates the function of creating a longitudinal patient record, and an accessible PHR for use by patients, and through patients, by providers and third-parties.
2. The PHR should not necessarily aggregate and archive all data, but be an access point or conduit to key elements of the data
3. Problems like physician fatigue and data overload need to be managed at source, and cannot be addressed by manipulating PHR design.

[17] Halamka, JD, Mandl KD, Tang, PC. Early experiences with personal health records. Journal of the American Medical Informatics Association : JAMIA, 15(1), 1–7. DOI: https://doi.org/10.1197/jamia.M2562

4. Innovation must be encouraged to develop competitive (and possibly open source) user-friendly PHR services.
5. If data storage is federated and linked through master references, additional clarification is needed to address situations when the provider ceases to exist (practitioner death, institutional insolvency, etc.); or the data “at source” are archived and offline. If all participants are expected to be online, all the time, the NDHB should articulate who will bear these costs.
6. The NDHB should articulate policies regarding access to data once the patient is deceased, or when the patient cannot provide consent (when unconscious, or critically ill).

2.3.ii.(c) : Health Master Directories and Registries

Key Issues: 1) The need for Master Directories to list all participants in the ecosystem cannot be overstated and is a commendable and necessary undertaking. The goal of creating a verifiable, updated and single source of truth for all personnel and institutions in the ecosystem is essential for the system to function well. However, this gate-keeping function will be hard (though necessary) to operationalise in India’s highly fragmented healthcare delivery system across allopaths, AYUSH providers, community health workers, mid-level providers, nurses, paramedics and so on.

2) We note that Registry and Directory have been used interchangeably in the document. It is recommended that this be reviewed for conceptual clarity.

3) The focus on NCD registries seems misplaced in this design architecture, which should be agnostic to disease or community-type. The architecture should allow for registries as varied as disease-specific registries (TB or heart disease); location-specific registry (if affected by local water-table toxicity, for example), or event-specific registry (Bhopal gas tragedy survivors, for example).

4) Data quality and accountability are likely to be higher if the registries are decentralised to the district or state, and accessed via APIs, for all the reasons of maintaining data at sources articulated above, and for avoiding single points of failure.

5) Stipulation D in the concluding section “Harmonising Current Facility Registry Initiatives” states that the format and structure of the (facility) identifier should be designed such that it does not allow deciphering of any information offline. This statement is not clear and requires clarification. It is unclear if this is to protect group identity. For example, knowing that patient X went to a TB clinic reveals his TB status. Identities of all query-generators and data controllers should be hidden when data flows through the system, irrespective of the nomenclature format. The Consent Manager will be the only entity that will authenticate flow after verifying identities and consent.

6) Clarification requested: Will NDHM subsume all information like National Health Resource Registry of CBHI, National Identification Number of MoHFW, the National Register of Clinical

Establishment under its own database? The key question is of course how these data will be updated and verified? Describe in further detail the timelines, incentives, budgets, and maintenance plans for directories and registries.

7) We also introduce here the concept of metadata-based registry federation. At every instance when relevant notifiable data are changed, the creation of (or modification of) the new metadata should be notified to all local registries that had previously subscribed to receiving such an event.

8) Registries, with a few exceptions like the National Cancer Registries maintained by Indian Council of Medical Research (ICMR) and the National Cancer Grid, have not been very successful in India. The NDHB should describe what the incentives, budget, and sustainability plans are for both, the registries and the master directories. The success of the National Health Resources Repository (NHRR) may help determine the feasibility of what is proposed here.

Recommendations:

1. The categories listed in Figure 2.1 in the NDHB could be simplified into providers and facilities. Consider the entire range of actors whose identities need to be maintained and updated.
2. The emphasis on NCDs, while a national priority, must be replaced by a more agnostic design. These specifics may be better articulated in subsequent implementation plans.
3. Family Identifiers, while culturally relevant in the Indian context, cannot be a prerequisite. It violates data minimisation principles as well as privacy.
4. Reference and pointers should also not be considered a given, and must adhere to the same principles of consent, transparency, auditability and reference indexing articulated in prior sections.
5. Consider maintaining decentralised registries.
6. Registries need to be constantly notified and updated (push or pull).
7. Need further clarification on Stipulation D.

Our response to other Master Data requirements are listed in Chapter 3.

2.3.iii : Layer 3: Technology Building Blocks

Table 2.2 : Anonymizer

Key Issues: 1) The NDHB describes the Anonymizer as an entity or function that will de-identify and or anonymise data from the Health Locker for secondary use. Assuming this is in reference to the PHR or Health Locker described in previous sections, the Anonymizer concept does not work if the PHR is constituted by reference links and not actual data, as it should. There are also large quantities of data that will sit at source, where they are generated, in labs, in pharmacies, in clinics, in hospitals and in the mobile devices of solo practitioners. All of these data should be available for secondary use (as permitted by the patient, and by law). A centralised anonymisation schema may not work.

2) We underscore the importance of anonymising data at or close to source. Currently, all too often hospital administrators and policy makers have inadvertent access to line lists of clinical data at source. It is imperative that anonymisation happen at source, and possibly at multiple stages along the way.

3) With reference to the statement "It is necessary to identify the use cases where each of these 2 processes [deidentification or anonymisation] has to be used, depending upon the degree of privacy required in each use case," it is our position that the decision whether to deidentify or anonymise does not depend on the 'degree of privacy required' but on the 'kind of data being processed'. Under current laws, all health data qualify as 'sensitive personal data' and requires the highest degree of privacy due to the associated risks from a breach.

4) Most, if not all, data referred to in this Blueprint will therefore automatically attract the privacy and data security provisions under the Information Technology Act, 2000 (and soon the Privacy Data Protection Bill (Act)). If a data processor does not want to be subject to these requirements, they may choose to securely and irreversibly anonymise their data instead.

5) It is therefore also important to note that the current state of the art process of de-identification and anonymisation are likely to fail in the near future, given the permanent nature of digital data and rapidly evolving AI tools.[18] Anonymisation also damages data and renders it less useful in the future. Anonymisation must therefore not be a substitute for consent but may be viewed as an inducement in addition to consent. Consent is not without its limitations. We elaborate on Consent and its limitations in subsequent sections, and submit that the NDHB may pursue instead a combination of data protection techniques (anonymisation, obfuscation, query-based access and so on), Consent and a strong Fiduciary obligation on the part of the data controller.[19],[20]
Evolving data protection laws will dictate the composition of this hybrid approach and define the contours of permissible use and time-limitation of data. Its ramifications on applying big data analytics, machine learning and AI technologies is discussed elsewhere.

Recommendations:

1. Aggregating all records in one place and then anonymising them is not a good idea.
2. Anonymisation must be done as close to the source as possible, for secondary use.
3. Secondary uses must be audited and subject to time- and purpose-limitation of data, whether or not the data are anonymised.

[18] Rocher L, Hendrickx J, de Montjoye YA. Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications* volume 10, Article number: 3069 (2019). Available on https://www.nature.com/articles/s41467-019-10933-3

[19] Takshashila Institution (Website). Discussion document- beyond consent: a new paradigm for data protection. 2017 July. Available on https://takshashila.org.in/discussion-document-beyond-consent-new-paradigm-data-protection/

[20]Takshashila Institution (Website). Takshashila policy advisory: a data protection framework for India.2018 February. Available on https://takshashila.org.in/takshashila-policy-advisory-comments-white-paper-data-protection-framework-india/

4. Even better, the secondary user should delete the data immediately after
5. use and ask for the deidentified data again if they need it. That keeps the
6. patient in the consent loop.
7. Anonymisation must not be assumed to be irreversible
8. Anonymisation must not be considered a substitute for consent, but an adjunct.

Table 2.2 : Consent Manager

Key Issues: 1) We continue our discussion about consent and anonymisation here. The NDHB must recognise that deviation from an explicit consent design will risk harm to the security and integrity of the entire system. Transparency and Auditability will allow the combination of anonymisation (term used broadly), consent, and fiduciary obligations to work in the interest of the individual.

2) Of note, Broad Consent is consent taken for future 'reasonably foreseeable' and 'non-commercial' research uses of the data in addition to the immediate purpose for which consent is given) There are several efforts globally on what broad consent looks like,[21] as are arguments in favour of subscription to or membership in communities where certain kinds of consent is implicit.[22] Individual patients should be able to inherit policy bundles from communities that they voluntarily choose. Patients must also be able to override or modify the policies so inherited. Any access to de-identified data is typically mediated through a gatekeeper with patient or community representation.

3) While we agree with the primacy of consent in this design, we also recognise the limitations of consent - where a growing body of evidence shows that consent is not entirely always understood.[23] Matthan argues that placing a fiduciary responsibility on the data processor protects the patient from harm that arises for uninformed consent, and to some extent allow third-party use where consent may not be possible. Others argue that such conditions where consent may not be possible can be addressed by enforcing **transparency and auditability** across the system.

4) Additionally, the MeitY Consent Architecture is heavily reliant on the Internet and smartphones. Technological adjuncts like network initiated Unstructured Supplementary Service Data (USSD) may also be considered.

5) On a specific observation in the paragraph on Consent Manager, the Blueprint notes that the framework applies to longitudinal data and vertical data "related to an episode." We find this distinction unorthodox and probably not necessary.

[21] Citi Program [Internet]. Final rule revisions: understanding broad consent; 2017. Available from https://about.citiprogram.org/wp-content/uploads/2018/07/Handout-2-Understanding-Broad-Consent.pdf

[22] World Health Organization (Website). Guiding principles for participatory health research. Available on https://www.who.int/ethics/indigenous_peoples/en/index7.html

[23] See B. W. Schermer et al, The crisis of consent: how stronger legal protection may lead to weaker consent in data protection, 16(2) Ethics and Information Technology (2014).

Recommendations:

1. The MeitY standard cited, only provides the technical specifications for recording electronic consent. A detailed consent policy must accompany the NDHB to clarify operational issues.
2. Such a consent policy must be based on explicit consent, and place a fiduciary duty on any data processing entity to protect the privacy and security of health data.
1. Any consent assumed to be implicit (or in rare cases, when waived) must be supported by transparency and auditability. And even if implied, it should be purpose- and time-limited; and revocable.
3. The NDHB should describe how purpose-limitation and time-limitation apply to data, whether identifiable, de-identified or anonymised.
4. The NDHB should also describe what the ability to revoke consent would look like, and how it would be operationalised.

Table 2.2 : Health Locker

We agree with the design we believe is being proposed here - that of shared and updated reference links, without aggregating data to a single repository, risking massive security breaches from a single point of failure.

The suggestion that small clinics (*including solo practitioners*) contribute to Health Locker ecosystem via authorised repository providers is important. This also allows for market-forces to offer competitive services addressing security, privacy and accessibility.

Again, we reference the HDAF design proposed by the NHS referred to in the introductory chapter of this Blueprint. The HDAF architecture would also allow patients to create more than one Health Locker, to seclude health events that may be sensitive, but irrelevant to their care.

Recommendations:

1. Prototype and test the HDAF model proposed by the NHS as the architecture that undergirds the PHR and consented access across various nodes in the health delivery ecosystem. Data Minimisation is key.
1. The proposal for using the design of the DigiLocker as the default intermediary needs some clarification. While it can certainly be one option, other options that may be provided by the states or the private sector should also be allowed.
2. The Health Locker must be designed to promote data minimisation. A reference link avoids having all data aggregated centrally and while there is the risk that poor connectivity will result in some remote data not being accessible from time to time, it also means we are not creating a repository that will become a single point of failure from a privacy and security standpoint.
3. The Blueprint is unclear on the scope of the Health Locker. It could host some or all of: "original" documents, a clinical database (personal EHR), an authorisation server, access logs, and a relationship locator service (the links). The open API must be designed to

support any of these even if all are not implemented in a particular Health Locker at the same time.

4. Further clarification on how the Health Locker will receive and share structured data is necessary. A simple import and export of pdf files will keep India in the dark ages, precluding patients from benefiting from third-party applications.

Table 2.2 : Health Information Exchange

HIE is often understood (although need not be so) in a centralised architecture (a platform or disparate systems integrated centrally), rather than operating in a federated and distributed manner. Centralising all authentication and authorisation for all patients, for all transactions, across the country seems unnecessary and unmanageable. We submit that authentication and authorisation capabilities be decentralised. Further clarification is needed on how the PHR and Health Locker solutions described above integrate with the HIE.

Table 2.2 : Health Analytics

Key Issues: 1) The section on Health Analytics needs significant clarification, in particular for the need for the technological layer to conduct analytics, as opposed to merely make the data analytics ready. Health data can be used for decision-making throughout their life cycle - initially at the time of generation, they are usually used to influence diagnosis, then management, then continuity of care, quality of care, efficacy of treatment, and so on. These data will need to be accessed at multiple points, and by multiple actors. Patients may want to access their data, and consent to use by third party apps for “analytics” that help them manage their treatment plan (say, in an app that measures and trends blood glucose levels to meals and medications); or a provider may want to query the database of all their patients to monitor their own practice trends (how many of my patients with cough do I tend to treat with antibiotics?), or an administrator may want to monitor compliance to clinical pathways (how many patients with chest pain in my casualty ward received aspirin on time?), or a state health department may want to monitor de-identified malaria smear results to monitor outbreak pockets to target vector-control interventions; or the central government may want to look at all their RCH data to look for utilisation trends across districts and states, or may want to make anonymised data available to academic partners.

The Analytics Block may best serve the function of offering de-centralised analytic services, and stipulating best practices for third-party use of data in compliance with evolving domestic and international jurisprudence. Specifically, the NDHB must articulate how these data will integrate with the existing research and policy ecosystems. The ramifications of such large datasets on clinical trials and genomics research are huge, and must be addressed upfront.
Processes such as Health Technology Assessment and Standard Treatment Workflow, both of importance to the insurance sector, should also be linkable to the Analytics Block.

2)Making data available for decision support systems entails not only the technical availability of data but corresponding transparency mechanisms that allow a granular understanding of the inherent biases that accompany every kind of health data set.[24,25,26] The risks of Black Box algorithms dictating care and access are real, and the Analytics Block would therefore need to articulate its policies on requiring transparency of algorithms and decision support systems built using data from this publicly supported ecosystem. [27,28] That being said, it is important to recognise that "evidence," for many of our accepted practices in medicine is not strong, and often "weak," and yet widely accepted.[29] Each society (or individual) will have to calibrate its comfort with accepting something that works without entirely understanding how it does.

Clinical Medicine is after all an open source practice, teachable and modifiable at the local level by licensed practitioners. There is to date little centralised certification of medical practices. Though standardised clinical pathways are gaining traction and have shown to be effective, trade secret algorithms including artificial intelligence and machine learning risk compromising fair care and care delivery.

Recommendations:

1. A centralised Analytic engine should not preclude decentralised analytic capabilities across the entire system
2. The Analytics Block should articulate the rules of engagement for data access by all possible providers, whether for public, private or commercial use, in compliance with existing and evolving domestic and international laws.
3. The use of health data for AI/ML applications must be regulated, whether by existing device regulators under the MoHFW, or by a new entity.
4. Explicit articulation of the inherent biases in all health data must be recognised, with strong efforts to educate providers, policy makers and patients, on both the potential of and limitations posed by automated decision support tools in healthcare.

[24] Young L. Computer scientists may have a mind of their own. IEEE Spectrium [Website]. 2015 August 21. Available on https://spectrum.ieee.org/tech-talk/computing/software/computer-scientists-find-bias-in-algorithms

[25] Simonite T. Probing the dark side of Google's ad-targeting system. MIT Technology Review [Internet]. 2015 July 6. Available from https://www.technologyreview.com/s/539021/probing-the-dark-side-of-googles-ad-targeting-system/

[26] Kirchner L. When discrimination is baked into algorithms. The Atlantic [Internet]. 2015 September 6. Available on https://www.theatlantic.com/business/archive/2015/09/discrimination-algorithms-disparate-impact/403969/

[27] Sweeney L. Discrimination in online ad delivery. Commun. ACM. 2013 May 01;56(5):44. doi: 10.1145/2447976.2447990.

[28] Editorial. Walking the tightrope of artificial intelligence guidelines in clinical practice. The Lancet. 1 (3). Pe100, July 01, 2019" DOI: https://doi.org/10.1016/S2589-7500(19)30063-9 but still hyperlinked to https://www.thelancet.com/journals/landig/article/PIIS2589-7500(19)30063-9/fulltext

[29] Topol E. Deep Medicine. Chapter Two: Shallow Medicine. Basic Books, New York. 2019.

Table 2.2 : GIS systems

The particular focus on this singular data point, essentially a location identifier for facilities, or potentially for other data, is not clearly understood. Geo-spatial analysis (and use) probably belong in the application layer.

2.3.iv : Layer 4: Application Building Blocks

We believe that the Application Layer is critical for seeding and scaling this system. It is through this layer that patient, providers and policy makers will see value in exchanging data. The Application Layer will allow public, open source communities and private enterprises to offer services that can potentially improve access and quality.

We expect to see exponential growth in lifestyle assistance, counselling, training and monitoring apps targeting patients with non-communicable diseases, mental health disorders, adolescent health challenges. These applications, while in their nascent stage globally can have a significant impact on workforce training, task-shifting, compliance, motivation, and peer-grouping. The NDHE can provide a platform for accelerating innovation in space, while enforcing strict protections against misuse of sensate data by prohibiting unauthorised tertiary use of data, and notice and transparency.

Recommendations:

1. The focus on Telemedicine or any digital health intervention requires concomitant emphasis on change management, with equal attention paid to training, support, skill upgradation, evaluation, iteration and maintenance.
2. NDHB must articulate policies, in congruence with existing and evolving domestic laws, that will define purpose- and time-limitation of data when third-parties (including commercial applications) seek to and access the NDHE.

2.3.v : Layer 5: Access and Delivery

The NDHB notes the prospects of a near universal coverage of all families in the country with smartphones. Recent studies have shown these numbers are much lower. A February 2019 Pew Study revealed that only 24% of the respondents had smartphones, while 64% had simple phones.[30] The Mobile First principle, while desirable, may inadvertently preclude large sections from participating in the envisioned digital health ecosystem. The delivery of all digital services via a smartphone will further widen the digital divide in India, concentrating services in urban and small-town India.

[30] Krishnan V. 25% of Indians have a smartphone, says Pew study. The Hindu [Internet]. 2019 Feb 8. Available from: https://www.thehindu.com/news/national/24-pc-of-indians-have-a-smartphone/article26212864.ece

Recommendations:

1. The Blueprint’s heavy reliance on smartphones is not advisable. On the contrary, the Access and Delivery layer, in addition to digital services, may want to consider an analogue adjunct, like a chip-based health ID card as both a redundancy, and a bridge to the future.
2. The system should allow for Proxies or Delegates to represent children, incapacitated adults, family members that share technology, or those that are digitally naïve.
3. The distinction between Layers 4 and 5 are not self-evident, since the web-portal and apps may also be considered applications built on the health data grid.

2.3.vii : Vertical Layer 2:
The Command, Control, Communication Centre (CCCC)

Key Issue: Disease surveillance and the maintenance of an outbreak response team the cornerstone of good public health emergency planning. It is unclear why or how this function which is currently shared between various departments at the local, state and central level, would be rolled into the jurisdiction of the NDHM, or whether such mission creep is desirable.

Recommendations:

1. The NDHM should not primarily undertake surveillance and response responsibility but make readily available APIs (or services) to state agencies to share data continuously or episodically, as dictated and permissible by law.

   The CCCC is better situated under the MoHFW, in collaboration with the National Disaster Management Authority (NDMA), State Disaster Management Authorities (SDMAs) and ICMR.

CHAPTER 3: STANDARDS & REGULATIONS

3.1. Objectives of Standards and Regulations

Key Issues: 1) Key stakeholders in India have long recognised that Standards are the foundation on which health data interoperability can be built. Yet, adoption has been wanting. As Standards are inherently voluntary, their adoption requires incentives or regulatory mandates, as we have seen around the world.

We note that the NHP-2017 had proposed that the National Digital Health Authority (NDHA) would define the regulatory aspects of health exchange. Assuming the NDHM replaces the NDHA, this chapter in the NDHB lists several standards, but not regulations. Without regulatory teeth, it is unclear how these standards will be adopted.

2) Furthermore, as Baker et al argue, it is important to evaluate and classify the readiness of technology specifications for national standardisation.[31] Citing the experience of the United States Office of the National Coordinator for Health Information Technology (ONC), they identified five criteria for evaluating the readiness of each of the 14 specifications to be adopted as a national standard:

1. Need (low, moderate, high)
2. Maturity of Specification (low, moderate, high)
3. Maturity of Underlying Technology (emerging, maturing, mature, declining)
4. Deployment/Operational Complexity (low, moderate, high)
5. Market Adoption (low, moderate, high)

3) The NDHB mentions Fast Healthcare Interoperability Resources (FHIR), Logical Observation Identifiers Names and Codes (LOINC), Systematized Nomenclature of Medicine Clinical Terms (SNOMED-CT) etc. - all relevant to clinical health information. However for the entire "health enterprise" to work effectively, there are other standards that may need to be adopted as well for Government to Citizen (G2C), Business to Consumer (B2C), Business to Government (B2G), and Business to Business (B2B) applications and services.

4) These standards must not only be documents published on websites, but available in machine interpretable formats (APIs, libraries etc). It is important to recognise that the era of the "document and publish" approach for Standards will not support current and evolving needs for Standards adherence.

[31] Baker D, Perlin J, Halamka J. Evaluating and classifying the readiness of technology specifications for national standardization. Journal of the American Medical Informatics Association [Internet]. Volume 22, Issue 3, May 2015, Pages 738–743, https://doi.org/10.1136/amiajnl-2014-002802

5) The NDHB must plan to provide technical support to assist individual and institutions to assert interoperability with their systems. We discuss workforce training and change management in subsequent sections.

Recommendations:

1. The adoption and maintenance of standards and software must be made mandatory for an entity to be included in the proposed digital health ecosystem.
2. In addition to FHIR, LOINC and SNOMED-CT, the Blueprint must also recommend the adoption of standards for different kinds of engagements such as G2C, B2C, B2G, B2B being enabled by this platform.
3. The master data requirements for drugs may include the adoption of standards developed by the Centre for Development of Advanced Computing (CDAC) as a SNOMED-CT extension with chemical names, generics, packaging info, language extensions.
4. And standards prescribed in the NDHB must be made available at a minimal cost or for free, in an interoperable format (e.g., Structured Query Language (SQL) and eXtensible Markup Language (XML) databases and semantic web Triplestores).
5. A national level terminology coordination mechanism must be instituted to harmonise between different terminologies. Quality benchmarks must be developed and embedded into the terminology maintenance cycle. This includes feedback loops from terminology users to the terminology creators.
6. The adoption of these standards must be encouraged through tools that facilitate the use of the terminology, awareness about benefits, and effectiveness in the real business (i.e. clinical) processes through proof of concept demonstrations.
7. The importance of Knowledge Services (Ontologies, Process Templates, Pathways, SOPs) is not clearly articulated.

3.3 Standard for Consent Management

Key Issues: 1) The Standard proposed for Consent Management is the “ISO/TS 17975:2015 Health Informatics - Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information,” which is behind a paywall and under review. It is likely to be replaced by ISO/NP TS 17975.(https://www.iso.org/standard/78395.html)

2) We submit that consent needs to be looked at carefully in light of new machine learning technologies, big data use, and phenomena such as consent fatigue and the inadequacy of informed consent. There is need to conduct a thorough review of all relevant existing and evolving laws that may have overlapping and sometimes incongruous impact on data exchange as envisioned here (for example, The HIV/AIDS Act 2017, The Mental Healthcare Act, 2017, DNA Technology (Use and Application) Regulation Bill, 2019, the PDP Bill, etc.).

Beyond the simple seek-consent-grant-access model, there are dangers posed by incomplete understanding of consent, or coerced consent. An accompanying legal policy framework to complement MeitY’s technical framework would be highly desirable.

3) Consent management should be decentralised to a patient-controlled open source component of the stack. This limits the need to communicate consent policies to the service providers implementing the open API.

4) MeitY's Electronic Consent framework is a means to obtain consent. It is useful in that any system that provides for digital data flows will benefit from having a log of all consents provided. However, much more work needs to be done in operationalising it in the context of medical data.

5) Consent may not be enough - especially at this age, when phishing, social engineering, and coercion using incentives is frequent and digital awareness, beyond mere digital literacy, especially amongst the vulnerable is low.

Recommendations:

1. Patients should not be asked to share their consent policies via API. Rather, the personal stack should include a standards-based authorisation service such as User Managed Access (UMA) that centralises the policy decision point and distributes the authorisation enforcement.
2. The statement that discusses “managing consent” may be rephrased to state that consent must be meaningfully obtained, ensured and upheld (rather than managed).
3. A sophisticated system is needed to effectively evaluate the implementation of the digital consent artefacts for core privacy principles such as data minimisation. MeitY’s consent specifications are inadequate for this purpose.
4. The recording of consent must not be exclusively reliant on Aadhaar, and alternatives to Aadhaar e-sign must be included in the NDHB. The consent policy must account for situations where proxy consent may be needed (for instance where the patient is unconscious).

3.4.a : Technical Interoperability

Key Issues: 1) The section on Technical Interoperability states that certain core datasets like the Registries would be managed centrally, and the bulk of the information relating to citizen/ patient health records would be maintained and managed in a distributed model, at regional centres or at the sites of the service providers. We are in agreement with this model, where data sits as close to the source as possible and de-identified and anonymised before they move, as defined by their use.

2) However, the statement, “The Central Repository of NDHB shall support only records conforming to standardised formats of content.” is confusing, as the federated architecture previously described should have no centralised repository of data, unless this statement is referring to metadata or reference indices.

3) We note that the integration reference model (IRM) in IndEA framework provides a generic reference, which would have to be completely customised for healthcare. Exploring other interoperability standards could be considered before mandating IndEA.

4) An important aspect of using Standards at scale is maintainability, accessibility and availability. Unfortunately, the Meta-data and Data Standards (MDDS) for Health have neither been adequately updated, nor have they kept pace with industry and digital health innovation. The lack of maintenance is particularly problematic with MDDS. For example, geographical codes are based on the 2011 census and not updated - there are no codes for Telangana.

Recommendations:

1. Explore the feasibility and adequacy of IndEA for this ecosystem.
2. Reconsider the use of MDDS Standards are they are not adequately maintained; and / or the NDHB must recommend that the MDDS define and maintain its concepts and elements, before they can be adopted for use in this ecosystem.

3.4.b : Semantic & Syntactic Interoperability (Content)

Key Issues: 1) Adoption of FHIR resources is a welcome decision. FHIR Release4 (R4) is not normative, although that should not be a deterrent. However, how the ecosystem will evolve and be updated to subsequent versions, especially normative, needs to be articulated. This is another factor in favour of retaining data at source. Exports of data to a central repository may need to be updated with very new version.

2) It is worth noting that unlike previous versions of HL7 standards, FHIR resources have a different maturity model. Only two resources, Patient and Observation, are normative (stable) in R4; the rest are less stable.

Recommendations:

1. Recognise FHIR maturity model limitations in the design of the NDHE, and plans for managing future FHIR versioning should be in-built to prevent hindrances in interoperability.
2. Specifically, consider including in Table 3.3 “Questionnaire,” “Questionnaire Response,” “Risk Assessment,” “Medication Statement.” “Composition,” and “Bundle” resources.

3.4.c : Content and Interoperability Standards

Key Issues: 1) International Classification of Diseases 11th Revision (ICD-11) has been released in 2018. Before mandating International Classification of Diseases 10th Revision (ICD-10), it may be worth considering the feasibility of mapping from SNOMED-CT to ICD-10 or ICD-11, and mandate that organisations all move to SNOMED-CT. This harks back to our initial plea to re-imagine what health data documentation in India will look here. It is the thoughtful adoption (and customised application) of these standards that will determine provider usability, wide scale adoption, quality of data and usability of the data. There are, as we know, over 75000 ICD-10 codes, including Z63.1 (problem with relationships with in-laws), V97.33 (sucked into jet engine), and W61.43 (pecked by a turkey).

2) SNOMED-CT is currently used in large (mostly secondary and tertiary) settings in digitally advanced healthcare systems. India has the opportunity to learn from the experiences of other nations: consider customising and contextualising the application of SNOMED-CT to Indian realities. In spite of it being officially supported by the government, adoption has been very slow for several years. While India may conclude that SNOMED-CT is after all appropriate given its widespread global adoption, what the minimal data set will be, and how this is determined will be important.

Recommendations:

1. FHIR resource list should also include “ImagingStudy,” “DocumentRef,” “Media,” and “Binary” in the interest of enabling transfers of patient information (DICOM images, PDFs).
2. Instead of ICD-10, the NDHB must refer to the ICD-11 update. A transition period may be provided to allow the transition to SNOMED-CT with temporary support permitted for ICD in the meantime.
3. Consider mapping of SNOMED-CT to ICD-11 codes and providing it as a service to all users in the system.
4. Consider, in a Regulatory Sandbox, testing the appropriateness and readiness of the proposed standards, in primary and community healthcare settings (refer to our recommendation on the Optimisation Vertical in Chapter 5.
5. Consultations must also be held with various non-governmental organisations working in the field to implement digital health technologies to ensure integration and seamless transition from previously existing systems on which their interventions are dependent.
6. The base FHIR patient profile would likely have to be extended or an India-specific FHIR patient profile created. The NDHB must also specify how the minimal dataset/indicators will be identified and on what basis.

3.5. Standards for Privacy and Security

Key Issues: 1) Clarification is needed on whether the Digital Certificates recommended in Table 3.5 will be the basis of identifying and verifying providers and facilities, and will be maintained by the NDHM.

2) The principles of immutability, versioning, non-repudiation, audit-log and patient control are important and must, as is recommended, be baked into the design.

3) While transparency and auditability is mandated, the onus of detecting breaches cannot be on the patient, or the POC alone. Clear obligations must be placed on all entities in the ecosystem with access to patient data to report any data breaches and violations of privacy, including notifying patients. With a number of data breaches of sensitive health information having been

reported in India in the recent past,[32,33,34] it is important that such obligations be placed on all data processors. Patients must be routinely notified when their data are accessed (as they are today with financial transactions).

Recommendation:

1. Given the growing number of big data breaches in the world today, it is advisable to have an active notification system in place, where users are notified of access to their health data, as they currently are with financial transactions. Larger data breaches should be reported to relevant regulatory authorities.

3.6 Standards for Patient Safety and Data Quality

Key Issues: 1) This section addresses the safety of equipment and has borrowed concepts from medical equipment safety. This is very limiting is scope. Patient safety in the digital ecosystem will need to be defined in terms of risks of denial or delayed care when authentication or infrastructure fails, non-availability of digital information during emergencies (power outages, for example), consequences on security, bodily integrity and mental health on account of breaches of sensitive data, and finally, harm that may be caused by non-transparent decision support pathways or black box algorithms.[35] We do not see standards listed for data quality.

Recommendations:

1. Formulate standards for patient safety and data quality in terms of the protections needed in light of misuse of data, or use of biased data, or unavailability of data, and so on.
2. The NDHB should also address safety of Health IT interventions across the lifecycle. Sittig et al point out that pre-implementation, it is important for safety mechanisms to identify and mitigate risks to patient safety. Once deployed, constant safety monitoring is important.[36] Clear regulatory pathways need to be established for adverse event and error reporting so that defective systems (and algorithms) can be repaired.
3. Further, the NDHB should state how patients can contribute to the process of improving the safety of the system by reporting errors and seeking redress.

[32] Perappadan B. Data thefts bid hits Ayushman Bharat. The Hindu [Internet]. 2019 April 28. Available on https://www.thehindu.com/news/national/data-theft-bid-hits-ayushman-bharat/article26968026.ece

[33] Ranipeta S. Medical data of Andhra customers leaked, 27 lakh orders shown on Anna Sanjivini site. 2018 June 18. Available on https://www.thenewsminute.com/article/medical-data-andhra-customers-leaked-27-lakh-orders-shown-anna-sanjivini-site-83274

[34] Cimpanu C. Indian govt agency left details of millions of pregnant women exposed online. 2019 April 15. Available on https://www.zdnet.com/article/indian-govt-agency-left-details-of-millions-of-pregnant-women-exposed-online/

[35] Price II WN. Black-Box Medicine. Harvard Journal of Law & TechnologyVolume 28, Number 2 Spring 2015.

[36] Sittig D, Wright A, Coiera E, Magrabi F, Ratwani R, Bates D, Singh H. Current challenges in health information technology–related patient safety. Health Informatics Journal. 2018 December 11. Available on https://doi.org/10.1177/1460458218814893

4. To establish standards for professional records would require a body like the Professional Records Standards Body (PSRB) of the UK, where clinicians and technologists collaborate to define standards for the content of clinical records.[37]

3.8 Enablers of NDHB

Recommendations:

1. Consider re-labelling standards and interoperability measures, *prerequisites*, not enablers. Without standards, the NDHB fails.
2. Please note the limitations of the MDDS mentioned above
3. The use of eSign may not be essential given the reference to the Consent Artefact throughout the document, except for specific use-cases like signing up for an insurance policy.

[37] Professional Record Standards Body [Website]. Available on https://theprsb.org/

CHAPTER 4: INSTITUTIONAL FRAMEWORK

Key Issues: 1) The Institutional Framework describes a comparative analysis of national organisations familiar with handling big data, and international experience with creating EHRs, and settles on the South Korean and UK experiences. It would be helpful to understand why these two systems in particular. There may be no perfect system yet. While the Australian EHR has been considered a successful endeavour by the World Health Organization (WHO), it too is mired in controversy over data security.[38]

2) The NDHB states that "given the sensitivity of health data involved, Government should have complete ownership of the proposed institution with flexibility to attract private sector talent at appropriate levels of implementation, with adequate safeguards." For this institution to be successful, we recommend that in general principles for setting up such institutions with functional autonomy and independence, be followed: 1) set up as a body corporate (with perpetual succession, a common seal etc), 2) specifications for composition, terms of appointment and removal of members and 3) obligations with reference to accounts, audits and annual reports. Financial autonomy is also desirable but may not be feasible here.

3) We note that Table 4.2 does not allow for the NDHM to have representation from several key stakeholders including patients, civil society groups, practising clinicians, and researchers, all of whom are most directly impacted by the institution.

4) This chapter clarifies the role of the NDHM as the sole fiduciary. We recommend exploring in further detail the merits and limitations of this model, as opposed to that proposed in the NHS of allowing multiple fiduciaries. We have addressed some of these differing views in earlier sections.

5) The document states that the NDHM will be formed to drive the NDHB. Consider instituting state counterparts for faster and contextually informed implementation, given the wide variation in health needs, capacity and outcomes among states.

6) We strongly urge you to reconsider the proposed architecture that relies heavily on a centralised government-built, government-provided solution, partly sustained by transaction fees (that are most likely going to be transferred to the patients). This ecosystem would be most sustainable if built in partnership with the open source community and a range of domain experts and public, non-governmental, and private actors, many of whom have tremendous contextual intelligence and can help accelerate innovation and scale.

[38] Stilgherrian. 900,000 Australians opt out of My Health Record. ZD Net [Website]. Available on https://www.zdnet.com/article/900000-australians-opt-out-of-my-health-record/

Recommendations:

1. Create an Advisory, or preferably a Steering Committee that ensures representation from civil society and the key participants in this system, including practicing clinical providers.
2. Develop and invite inputs on a Change Management Plan for seeding and scaling the human resource capacity across all involved sectors.
3. The Financing Model, albeit scant now, should include costs for maintenance, enhancement, infrastructure (hosting, network), research (prototypes, trials), training, education, etc.
4. Consider creating a Prototyping Building Block (in conjunction with a Regulatory Sandbox) to test alternative models, allow rapid iteration, and provide interoperability testing labs. This will allow the NDHB to test critical elements of the technology platform (specifically the PHI, the PHR and Health Locker), before adopting or mandating them en masse.
5. Expand the architecture to permit participation by other actors, while retaining core elements essential to security, privacy and service delivery. Build in safeguards against regulatory capture.

CHAPTER 5: NATIONAL DIGITAL HEALTH MISSION ACTION PLAN

5.1. Purpose of NDHM Action Plan

Key Issues: 1) Some of the building blocks have been described in detail. Architectural details for the others need to be articulated, as well as the relevant regulatory frameworks. The rationale for the building blocks of Social Media and Call Centre are not entirely clear as the former is a communication strategy for public outreach or notification, and the latter is a very specific service that should perhaps be decentralised (to be contextually relevant), specialised, and integrated with the NDHB like any other service in the system (hospital, clinic, lab, public health agency, etc.)

2) The stipulation that citizens undergo diagnostic tests only once is aimed at minimising waste and redundancy in medical testing, resulting from lack of data portability. Yet, a stringent criteria should not result in any onerous burden on provider, payer or patient when repeat testing is clinically warranted. What would be the means of monitoring, validating, preventing or penalising such action? Providing burden of proof through additional documentation for each instance of repeat testing can slow care down. In-patients often need the same lab test repeated several times a day, some tests are to be periodically repeated (like International Normalised Ratio (INR) checks for anticoagulant therapy), and some radiological imaging may need to be repeated for better resolution. Exhibit caution while developing any such criteria for permitting (or prohibiting) repeat testing.

It is not clear why the NDHB can, or indeed whether it should, attempt to influence practice patterns in this way, other than by providing the data infrastructure required by the respective professional societies or ministries to set policy.

3) Further clarification is requested on the statement, “ Citizens should get Integrated Health Services at a single point, though multiple agencies/ departments/ services providers are involved”

4) Further clarification is requested on the National Health Portal. Will this be the same as www.nhp.gov (2013), or a new one?

5) Further clarification requested: Under which ministry is the budgetary allocation planned, possibly the MoHFW?

6) We would like to note again there NDHB must address grievance redressal for incorrect data, data breaches, consent avoidance, privacy violations, denial or delay of service and, non-transparent automated algorithms.

7) The NDHB is light on details about the system of incentives for adoption - which is critical to the success of this entire enterprise. The discussion on incentives must also be accompanied by well-planned timelines for workforce training.

8) We believe that a bold and ambitious plans such as this, likely unprecedented at a global scale, warrants a strong implementation science component: a) to test (preferably within a Regulatory Sandbox, and rapidly) every building block proposed here; b) to measure and monitor outcomes, including privacy impact assessment; c) and to provide grievance redressal to all users of the system. We include grievance redressal here so that during these early stages of development, the grievances are not seen as on-off cases, but signals for possible system-wide weaknesses that need urgent rectification.

9) The NDHB must recognise ground realities observed during rollouts of recent national digital health interventions: Given the poor connectivity, low awareness of both care providers and beneficiaries, and overburdened staff, compliance to the required digital processing during enrolment, consent, and service provisioning has been challenging, though expected to improve incrementally. This slow ramp up also affects quality and interpretability of data.

9) It was our unanimous consensus that the timelines published here are overly ambitious and preclude the NDHB from being responsive to real-time feedback. We recommend harnessing the desired rapid pace to quickly testing multiple prototypes for picking the model best suited to the Indian context. This is a colossal enterprise, embarking on largely uncharted territory (at this scale). Its importance should not be trivialised by suggesting that implementation will take a fraction of the time taken by all others.

10) The NDHB may want to consider a phased rollout where all care delivery nodes are divided into the three tiers, where the first tier includes institutions it can most influence by incentive or mandate, for example, all teaching medical colleges and health facilities under the purview of the MoHFW. The second tier would extend to nodes that users of the public system most frequently interact - namely chemists and diagnostic centres. The third tier would include the rest.

A better articulation of incentives is necessary, in the next iteration. Will institutions and personnel both be incentivised? What are the estimated costs, and who will bear the burden? Consider reducing the expected adoption-friction by investing upfront in consensus building and human-centred design.

11) Significant portions of our most vulnerable populations - migrants, rural and remote communities, child laborers, etc. are cared for by long established non-governmental organisations, many of whom are well integrated into the public health delivery system and have even been at the cutting edge of scientific breakthroughs in primary care medicine, delivered through cadres of well-trained community health workers: Jan Swasthya Sahyog (JSS), Piramal Swasthya, Sangath, MAHAN, Karuna Trust, SEARCH, and a myriad of smaller players. Many such actors that straddle both the public and private sector have large (and often meticulously maintained) databases, sometimes in non-standard media and formats. It would be important for the NDHB to articulate a plan for bringing these players on board, whose make a large contribution to care delivery to the most vulnerable.

Recommendations:

1. The intention to guarantee a user-friendly interface is desirable, but the “5-click” stipulation seems arbitrary. 5 clicks on a slow internet connection, for example, would seem like an eternity. The emphasis should be on insisting on user feedback loops during the design process, rapid prototyping, and testing, before large-scale roll-outs.
2. The NDHB should not directly dictate clinical practice, but provide the data infrastructure required by administrators, scientists, professional societies and practitioners to formulate policies.
3. We recommend creating an “Optimisation” vertical that includes the Prototyping Building Block introduced in Chapter 4, with other mechanisms to allow for continuous feedback loops, and grievance redressal, to optimise the system’s performance to meet its articulated vision.
4. Is the Unified Communication Centre same as CCCC or the call-centres? We recommend that these be considered services that plug into the NDHB, but not be administered by the NDHB.
5. The timelines stated look very ambitious. The NDHB is comprehensive and has the potential for several long-term benefits. It may be worth taking the time to rapidly prototype (perhaps even simultaneously) the various designs proposed in the document - many of which have not been tried in the Indian context.
6. Consider reviewing the sequence of items in the ‘Artefact Deliverables’ section on page 45. For example, NDHB Security Policy and NDHB Privacy Policy may have an impact on the development of a Federated Enterprise Architecture and may need to be moved up the list. Till legislatively backed protections under the Personal Data Protection Act come into effect, it should be ensured that this Security and Privacy Policy provides effective safeguards that mirror the proposed law and are enforced by the NDHM.
7. Consider a Change Management vertical with careful attention not only to initial workforce training, but also to sustained support, re-training and skills upgradation. The concept of clinician or administration champions to drive change locally (within institutions or departments) has been very successful in other contexts. In India, state level champions have been key to successful at-scale implementation (eg. ImTeCHO)
8. Articulate a policy for supporting adoption, integration, training and infrastructure upgradation for the non-governmental organisations that are delivering care at scale.
9. Consider a tiered approach by prioritising delivery nodes that the NDHB can most easily influence, and monitor.
10. Please consider posting all responses the NDHB receives publicly in the spirit of fostering cross-pollination of ideas. We all stand to benefit from each other’s perspectives.

We thank the Ministry of Health and Family Welfare and the Shri J Satyanarayana Committee for this opportunity to allow public comment on this very important document.