

Policy Proposal

Reimagining Health Data Exchange: An Application Programming Interface–Enabled Roadmap for India

Satchit Balsari^{1,2}, MD, MPH; Alexander Fortenko³, MD, MPH; Joaquín A Blaya⁴, PhD; Adrian Gropper⁵, MD; Malavika Jayaram⁶, LLM; Rahul Matthan⁷, LLM; Ram Sahasranam⁸; Mark Shankar⁹, MD; Suptendra N Sarbadhikari¹⁰, PhD; Barbara E Bierer¹¹, MD; Kenneth D Mandl^{12,13}, MD; Sanjay Mehendale¹⁴, MD, MPH; Tarun Khanna⁹, PhD

¹Beth Israel Deaconess Medical Center, Harvard Medical School, Department of Emergency Medicine, Boston, MA, United States

²Harvard FXB Center for Health and Human Rights, Boston, MA, United States

³New York-Presbyterian Hospital, Emergency Medicine, New York, NY, United States

⁴The Human Diagnosis Project, Washington DC, DC, United States

⁵Patient Privacy Rights, Boston, MA, United States

⁶Digital Asia Hub, Hong Kong, China

⁷TriLegal, Bangalore, India

⁸Athenahealth, San Francisco, CA, United States

⁹Harvard Business School, Boston, MA, United States

¹⁰International Institute of Health Management Research, New Delhi, India

¹¹Brigham and Women's Hospital, Harvard Medical School, Boston, MA, United States

¹²Boston Children's Hospital, Computational Health Informatics Program, Boston, MA, United States

¹³Harvard Medical School, Department of Pediatrics and Department of Biomedical Informatics, Boston, MA, United States

¹⁴Indian Council of Medical Research, New Delhi, India

Corresponding Author:

Satchit Balsari, MD, MPH

Harvard FXB Center for Health and Human Rights

651 Huntington Avenue, 703C

Boston, MA,

United States

Phone: 1 6174320011

Email: sbalsari@bidmc.harvard.edu

Abstract

In February 2018, the Government of India announced a massive public health insurance scheme extending coverage to 500 million citizens, in effect making it the world's largest insurance program. To meet this target, the government will rely on technology to effectively scale services, monitor quality, and ensure accountability. While India has seen great strides in informational technology development and outsourcing, cellular phone penetration, cloud computing, and financial technology, the digital health ecosystem is in its nascent stages and has been waiting for a catalyst to seed the system. This National Health Protection Scheme is expected to provide just this impetus for widespread adoption. However, health data in India are mostly not digitized. In the few instances that they are, the data are not standardized, not interoperable, and not readily accessible to clinicians, researchers, or policymakers. While such barriers to easy health information exchange are hardly unique to India, the greenfield nature of India's digital health infrastructure presents an excellent opportunity to avoid the pitfalls of complex, restrictive, digital health systems that have evolved elsewhere. We propose here a federated, patient-centric, application programming interface (API)–enabled health information ecosystem that leverages India's near-universal mobile phone penetration, universal availability of unique ID systems, and evolving privacy and data protection laws. It builds on global best practices and promotes the adoption of human-centered design principles, data minimization, and open standard APIs. The recommendations are the result of 18 months of deliberations with multiple stakeholders in India and the United States, including from academia, industry, and government.

(*J Med Internet Res* 2018;20(7):e10725) doi: [10.2196/10725](https://doi.org/10.2196/10725)

KEYWORDS

health information exchange; India; health APIs

Introduction**Background**

India's population of over 1.3 billion is served by over 2.5 million health care workers of varying qualifications. The vast majority of clinical interactions are not digitized. In the few instances that they are, the data are not standardized, not interoperable, and not readily accessible to clinicians, researchers, or policy makers [1]. While barriers to easy health information exchange (HIE) are hardly unique to India, the greenfield nature of India's digital health infrastructure presents an excellent opportunity to avoid the pitfalls of complex, restrictive, digital health systems that have evolved elsewhere.

In February 2018, the Government of India announced a massive public health insurance program under the National Health Protection Scheme (NHPS), offering Indian Rs 500,000 (approximately US \$ 7,600) in annual coverage to 100 million households, or nearly 500 million citizens [2]. To meet this bold target, the government will rely on technology to effectively scale services, monitor quality, and ensure accountability. While India has seen great strides in informational technology development and outsourcing, mobile phone penetration, cloud computing, and financial technology, the digital health ecosystem is in its nascent stages and has been waiting for a catalyst to seed the system. The NHPS is expected to provide just this impetus for widespread adoption.

We propose here a federated, patient-centric, application programming interface (API)-enabled health information ecosystem that leverages India's near-universal mobile phone penetration, universal availability of unique identification (ID) systems, and evolving privacy and data protection laws. The arguments laid out here are the result of an extended set of deliberations that began at an interdisciplinary seminar held at Harvard in September 2016 and have since resulted in potential pathways for prototype development in India.

The State of Health Data Exchange

Electronic Health Records (EHRs) have traditionally been closed systems, sometimes incapable of sharing access across platforms within the same institution, and almost never across vendors at independent institutions. While more systems now allow patients access to their health-related data, few EHRs give patients control over how their data will move across institutions or be shared between providers. Despite significant legislation, a large portion of health data collected today remains inaccessible due to legitimate concerns over confidentiality and privacy, risk-averse hospital policies, prohibitive costs associated with change, and inertia [3].

While health data have been typically associated with information captured in EHRs, there is growing recognition that data are generated at multiple nodes along the delivery system. For example, at the pharmacist, at the stand-alone imaging facility, at the laboratory, at the general practitioner's office, at the hospital, at the insurance company, and now, even on one's

wrist [4]. However, the lack of standardization among data storage systems makes it virtually impossible to combine and collate data from multiple sources, resulting in duplication, redundancy, wastage, and delays [5].

The concept of a personal health record (PHR) has long been floated as one potential solution to disjointed health care data [4,6,7]. A PHR relies on a patient-controlled repository where data may be accessed from multiple nodes within the system. Standalone PHRs mostly rely on the patient's drive and ability to input data [8,9]. Tethered (ie, connected) PHRs are patient-accessible components of electronic medical records linked to an institution or health system [8,9]. Still, there are drawbacks. PHRs seldom allow direct input from or access to entities outside the network. Neither PHR model allows for the development of third-party applications (app) on the patient's health data repository. Although there is interest from the consumer, widespread adoption of both has been hindered by concerns about data ownership, interoperability, security, and scalability [10-12]. The Ministry of Health and Family Welfare (MoHFW) in India has demonstrated an interest in developing a PHR-based system [13].

In recent years, additional individual and population health data have been generated by wellness gadgets (eg, Fitbit), Web-based diagnostic devices (eg, AliveCor), patient-facing apps (eg, Stanford Healthcare), provider-facing apps (eg, Practo), or researcher-facing apps (like Apple's Research Kit). These new apps and gadgets create additional silos of health data. In fact, of the 260,000 mHealth apps that existed on the last count, 90% were free—their financial viability predicated on their ability to monetize the data they collect [14]. In the United States (US), the 21st Century Cures Act (2016), mandated that “certified” health information technology (IT) products have APIs that allow health information to be accessed, exchanged, and used “without special effort.” Standardization was not mandated, making interoperability difficult to implement [15]. In India, while the mHealth industry is booming and expected to grow exponentially, there are no legal provisions to regulate access to personal health data that flow in and out of these devices and apps, and sometimes across international borders [16].

The call for data integration, universal compatibility, and portability has come from many quarters. There is no shortage of standards, but few are universally applied. There are standards for nomenclature and terminology, structural and semantic standards, and open source technology platforms that promote secure health information exchange [17]. Entrepreneurs and provider networks have responded to this need for data portability, and the potential for monetizing vast amounts of data, by creating their own ecosystems where the patient is not the final arbiter of data flow [18-21].

There is now sufficient recognition that restricting health data access is detrimental to patient care, provider satisfaction, and health care costs [22]. Conversely, access to health data has been shown to benefit and empower patients [23]. Authorized access to the vast troves of accumulated digital data helps

accelerate medical research [24]. In March 2016, the US National Institutes of Health in collaboration with the Office of the National Coordinator for Health IT announced the launch of the Precision Medicine Initiative Sync for Science program. Based on existing community standards and specification efforts, this pilot program gave patients easy access to their data and allowed them to donate it to researchers [25] securely. The most significant challenges facing this initiative are individual and collective concern over data security and privacy, and hospitals' and practitioners' reluctance to promote the program.

Health Data in India

Health is a "state" subject in India, managed and funded by state governments, with part-funding from the Center (ie, the federal government in Delhi). Consequently, there is wide variation in quality of care within and among states [26,27]. On average, 70% of health care is delivered through the private sector, which is comprised of state-of-the-art tertiary facilities, nursing homes, polyclinics, general practitioners and a large workforce of health care providers with no medical qualifications [28]. The public health system is robust in population health interventions like vaccine delivery but struggles to provide quality primary care or specialized services at scale [29]. There are also stark differences in health care services in rural and urban India, with the majority of the medical workforce, and tertiary services gravitating to urban India [30].

Conversations about health information exchange in India must acknowledge these realities, as well as the near absence of digital health information in most clinical transactions. The private sector is mostly not digitized except for major diagnostic laboratory and radiology franchises, and some private hospital networks [31,32]. Hospital chains like the Apollo Group and Max Healthcare Group with advanced EHRs have reached Stage 6 of the Healthcare Information and Management Systems Society classification of EHR adoption [33]. However, EHRs are not yet portable across these institutions, and most systems continue to struggle with physician compliance [31,32,34].

In the public sector, data have been collected through various overlapping, regional or national mandates, or dictated by the needs of sponsoring philanthropic foundations [35-37]. The systems, where they exist, are District Health Information System 2 compatible, and mostly comprised of aggregate data. Longitudinal patient records are a recent (and still rare) phenomena. Select public hospitals have managed to digitize some components of the medical record. The governments of Rajasthan, Andhra Pradesh, Maharashtra, and Tamil Nadu have all sponsored EHR implementation to varying extents [38,39]. The Tamil Nadu system, for example, connects over 1,500 primary health centers, 267 secondary care hospitals, and 17 medical colleges. Sustained investment by the state government has been key to the program's success and scale [39]. The JJ Group of Hospitals in Mumbai, Maharashtra has logged over 20 million patient visits in the past decade, using the Amrita HIS platform [40]. India's premier public hospital in Delhi, AIIMS, uses a patient scheduling software aimed at reducing wait times. Several other state government sponsored tertiary hospitals use the e-Aushadhi supply chain management system [41,42]. However, these systems lack portability. They are also

limited to government-run health facilities precluding residents from accessing data across state lines or from transporting data across public, and private health care facilities.

At the primary care level, community health workers and clinical staff log data in paper-based notebooks, tablets, excel sheets, and a variety of software applications that differ from state to state. The validity of much of these data is questionable [43,44]. Preliminary analysis from a study by our team at a primary care center in one state in India shows that there are over 3,000 discreet fields of data captured in paper-based and electronic forms, contributing data to 70 different databases, the majority of which are never accessed or used for real-time clinical or policy decision making. These repetitive data collection requirements result in large duplication, wastage, and divergence of limited human resources.

Health data are also captured at hundreds of research institutions across the country, in paper files, personal flash drives, hard drives, and sometimes on institutional servers. There is a general consensus among local researchers that much of these data are never analyzed, and they seldom change clinical practice or care delivery [45,46].

Data do not travel across jurisdictions. For example, the Indian Council of Medical Research, India's leading body for biomedical research has limited access to the data generated across its various collaborating institutions, and almost none to data generated in private institutions. Critical clinical data with significant individual and public health consequence, like information on compliance and antibiotic resistance, are not portable across institutions. Also, the government's Revised National TB Control Program cannot follow patients or monitor their care once they choose to seek treatment in the private sector. Even if private sector entities were willing to share data, there are no mechanisms to do so. The lack of interoperability of such critical data has a profoundly negative consequences on existing disease surveillance systems [47].

There is growing recognition among the public sector that all new digitization efforts must conform to prescribed standards. The government adopted Systematized Nomenclature of Medicine (SNOMED) and is making it available free of cost to health systems across India [48]. Organizations like HIMSS and the India Health Information Network are other key stakeholders. While the government intends to establish interoperability standards, the question of change management remains unaddressed. Who will bear the cost of these new systems, and of transitioning the older systems? What will be the institutional and individual incentives? How will the system be seeded, populated and sustained? In the United States, the Health Information Technology for Economic and Clinical Health (HITECH) Act provided incentives (and penalties) for Electronic Health Record (EHR) adoption, at the cost of US \$ 34 billion in payments to doctors and hospitals to purchase and promote electronic health systems [49]. A 2017 study comparing hospitals that qualified for monetary incentives for implementing "meaningful use" of EHRs to those that did not qualify, attributed 8 percentage points in adoption growth to the incentives provided by HITECH [50]. India can barely afford such expenditures when health spending is at less than 2% of

its GDP [51]. What then would be the much-needed catalyst to stimulate widespread digitization?

Until 2017, the lack of a significant insurance player in the market precluded piggybacking EHR adoption on the billing requirements of payers and providers. Deliberations with critical stakeholders in India facilitated by the authors through 2016 and 2017 focused on the three nodes in the system that were most digitized, namely, laboratories, pharmacies and radiology reports. Still, mechanisms for change were not clear. The 2018 NHPS, with its urgent need for a technological backbone, changes all that—it has potential to finally develop this vision for universal HIE in India.

This approach is, however, not without its dangers. The EHRs in the United States have evolved as very effective billing instruments and provided medicolegal safeguards, but basic patient and provider needs like portability and access were an afterthought and required prohibitively expensive retrofitting. Systems work best, and compliance is highest, when the EHRs can be customized to local workflows, and when they can be modified or upgraded with relative ease and at low costs. Hospital mergers in the United States have resulted in near-uniform systems across vastly different enterprises, changes in which require universal consensus across the ecosystem and entail prohibitive fees charged by EHR corporations and additional re-training costs.

While the NHPS may indeed be the much-awaited catalyst for jumpstarting the digital health ecosystem in India, mandating a one-size-fits-all nationwide billing platform will do irreparable and costly damage—costs the Indian health care system cannot afford to bear [52].

An Application Programming Interface–Enabled Health Information Exchange for India

Between August 2013 and December 2016, India's MoHFW released a set of recommendations for electronic health records that outlined vital components of a standardized health care information ecosystem, and a common language for the organization of medical terminology and data [43,53]. The Ministry also instituted the National Digital Health Authority meant to “regulate, develop and deploy digital health along the continuum of care across India [54].” In December 2016, the government's Centre for Health Informatics released a Request for Proposals for the creation of an integrated health information platform (IHIP), where the exchange would be facilitated via a central storage repository. Low budget allocation and limited information on the proposed architecture precluded most IT service companies from bidding. The contract was finally awarded in January 2018, just weeks before the NHPS was announced [55]. The centralized IHIP as envisioned would be monolithic and prescriptive, risking poor user adoption, high physician burnout, and little meaningful access to the vast data it would generate, as seen in large hospital systems in the United

States [52,56]. It risks not being able to leverage future IT developments.

The prototype outlined below argues against the use of a centralized repository of health data. Instead, we submit that the way forward must be an API-enabled, blockchain-based information network in which the personal health record underpins a system where free, real-time flow of data is predicated on consent and authorized access. India is uniquely positioned to build this ecosystem armed with a universal identity system, experience with digitization across multiple other industries, and a sophisticated domestic IT workforce.

We describe below the technical and legal basis for the design proposed.

Federated Architecture

Our proposed model calls for a federated architecture that acknowledges current and future health information flow; for example, between providers and patients, wearables and EHRs, consumers and pharmacies, physicians and laboratories, or institutions and payers. Collating all data in a national repository for 1.3 billion Indians will prove to be prohibitively expensive, redundant, and wasteful. It would also offer a single point of failure where security breaches would result in colossal data compromise. A federated system would allow data to sit at the source and be recalled on demand.

An API-enabled federated health data architecture would function on blockchain principles as an “open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way” [57,58]. Consider a PHR that could query all nodes in the network to receive periodic updates—from wearables, diary entries, pharmacists, doctors, hospitals, diagnostic labs, imaging facilities, and payers. It is possible to map out various permissible pathways through which the data can travel automatically while there may be others through which it cannot pass without the patient's consent (Figure 1).

An authorized physician—even a virtual “teledoc”—would be able to call for her patient's entire record, either through pre-authorization, real-time authentication, or waivers in case of emergencies [56]. Diagnostic laboratories should be permitted to send their reports to the patient's physician who requested the test but will need authorization from the patient to send it to any other doctor (such as one to whom the patient goes for a second opinion). Similarly, a public health agency, duly authorized, should be able to query select de-identified test results across all laboratories in a region of interest, to forecast, monitor, and respond to disease outbreaks [59]. Health system administrators should similarly have access to aggregate data for monitoring delivery, resource utilization and clinical outcomes. Physicians should be able to query their practice patterns. Third-party applications that are built off the patient's PHR, for example, alerting the patient to vaccine requirement before travel, or triggering reminders based on her medication list, would need the patient's permission to access data from her PHR (Figure 2).

Figure 1. Federated Health Information Exchange Schema: The personal health record (PHR) would access data from existing and novel sources, by preauthorization, waiver or legal mandate. EHR: electronic health record; MOH: Ministry of Health.

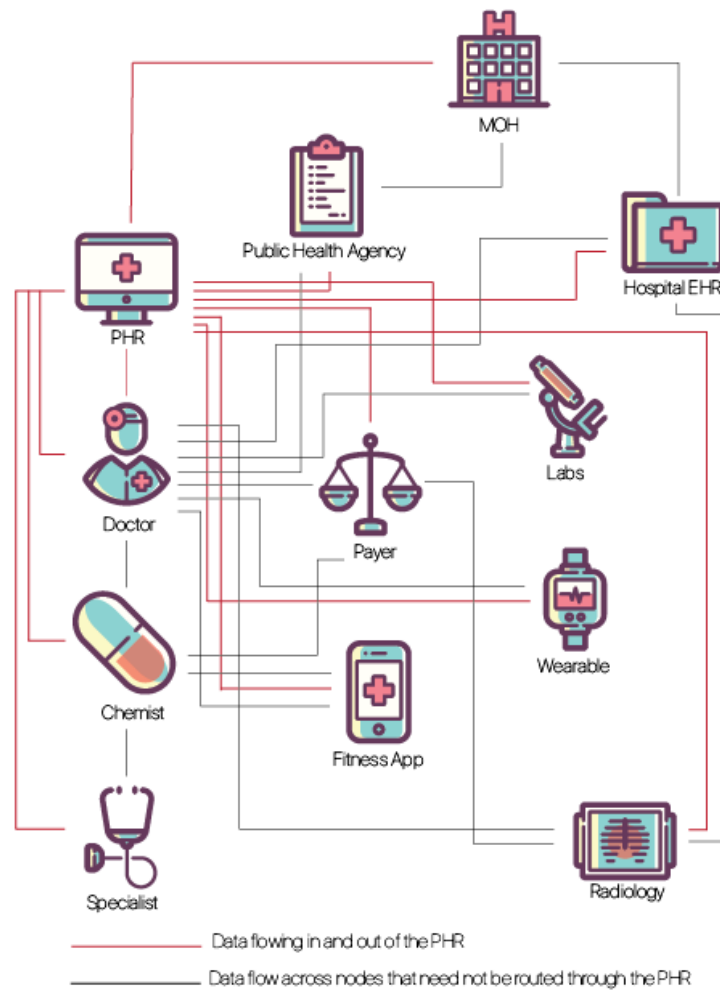
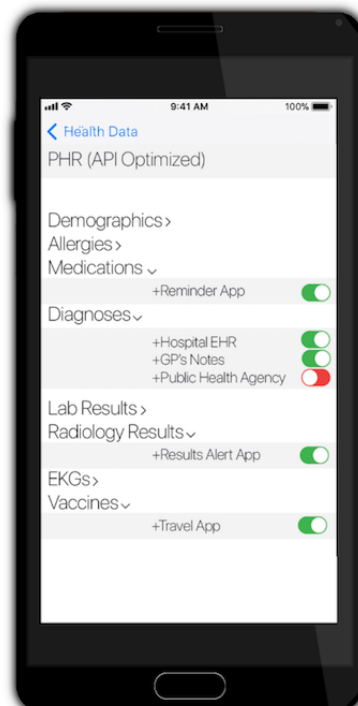


Figure 2. A customizable personal health record (PHR) interface. Through user-driven consent and control, third-party plug-ins (apps) can access the PHR via standard open application programming interfaces (APIs).



As long as the user is “recognized” by the system, and therefore has pre-authorization to query particular types of data, access should be easy and near instantaneous. Essentially, the “consent” process is separated in time and place from data flow, allowing timely, secure, exchange of relevant health data between nodes. A federated and distributed network so constructed would obviate the need for constructing large national or regional databases of the patient’s “entire” medical record. Opportunistic synchronization and personal device-based back-up may reasonably mitigate the effect of unreliable electricity and connectivity. Moreover, all these inquiries and interactions should generate audit trails to prevent misuse.

Smartphone penetration in India is expected to reach about 36% of all mobile phone users [60]. While important components of the proposed architecture, mobile phones are not critical. Web-based services, hospital-based kiosks, and patient service facilities can assist those without mobile phones in understanding and accessing their settings. Local regulations should ensure that the default always protects the patient’s interests and privacy.

While seemingly simple in architecture, such a system is predicated on standardization and widespread adoption. We next discuss how there is sufficient precedence and local capacity to favor such sweeping change.

Universal Unique Patient Identifier

Prima facie, access to the federated architecture would require a universal identifier. All data would be tagged with that unique identifier no matter where the patient interfaced with the medical system. Further, any entity contributing to or extracting from the system would need a unique institution and personal identity tag.

While usually a daunting system to create, the near universal penetration of India’s unique biometric identification program, Aadhaar, offers a solution to this challenge. Aadhaar has been built around the principles of privacy by design, and data minimization, that are particularly relevant in security-sensitive applications like health care. Administered by the Unique Identification Authority of India, the system is actively used today for the central government’s direct benefit transfers and subsidies programs and has also been used by several banks and telecom operators. By 2017 over a billion Indian residents were enrolled in Aadhaar, making it the most widely deployed single ID system anywhere in the world.

This astonishing penetration notwithstanding, mandating the linkage of public services to Aadhaar has been problematic, and a subject of constitutional challenges before the Supreme Court, with legitimate concerns of misuse and state overreach [61]. It is possible that the public resistance for using Aadhaar may necessitate the creation of a separate unique medical identity number.

Local Precedence

The use of APIs would underpin the proposed federated architecture. An API is a set of routines, protocols, and tools built into a software application that enables it to communicate easily with other applications. APIs provide the means to build

interoperable software and data exchange services. APIs are already behind the seamless integration from which we benefit every day. They allow Instagram to access the camera on our phones, agnostic to the maker of the device; or allow WhatsApp to access our phone directory (“contact lists”); or a taxi app to use Google maps. Industries like banking, finance, and social media have already successfully tapped into the explosive growth of software applications by adopting API-based solutions [62,63]. Unrelated corporations own most products that communicate via APIs, yet the use of standard APIs powers the entire digital ecosystem.

India’s own experience with wide-scale API adoption in the financial technology (eg, fin-tech) sector has been regarded as hugely successful: The Unified Payments Interface, rolled out in 2016, has demonstrated both the feasibility and the advantages of adopting an API-based ecosystem. Aadhaar spurred a range of nationwide API-based IT solutions, collectively referred to as IndiaStack [64]. The Aadhaar dashboard eKYC, for example, is a paperless “Know Your Customer” (KYC) process aimed at verifying an individual’s identity. This instant electronic verification has replaced the traditional KYC process that relied on the onerous in person presentation of paper-based copies of official identity documents. The eKYC is currently used across many industries, including banking, utilities, and mobile services, and has logged 4.2 billion transactions in the past four years [65].

The Digital Locker is another successful application that provides a cloud-based storage service to all residents that authorized users can access. Registered Digital Locker organizations can push (or retrieve) electronic copies of documents and certificates (eg, driving license, voter ID, school certificates) directly into the lockers of Indian citizens, once again making credentialing and verification processes near-instantaneous. As of January 2018, nearly 2 billion digital documents have been issued through the Digital Locker API [66]. The widespread adoption of these changes in the financial-tech sector was catalyzed by support from the highest levels of government.

The successful and explosive use of mobile financial services notwithstanding, user-controlled dataflow through the federated network assumes some degree of digital literacy and understanding the ramifications of consent, secondary data use, artificial intelligence algorithms, and so on. Until such time that the Indian populace is assumed to have such knowledge, concomitant local laws will need to require that default data access protects foremost, the patient. We discuss the relevant existing and evolving Indian legal standards in subsequent sections.

Global Standards

Globally, the health care industry has begun embracing API-based exchange. Open Medical Record System, and platforms like SMART Health IT, developed at Boston Children’s Hospital, have long pursued health data ecosystems anchored in open standard APIs [67,68]. These programs, while successful, had been limited in scale due to the rigid and expensive architecture discussed above. However, the field is rapidly changing. In June 2017, Athenahealth invested US \$63

million in a product that improved user-experience and ensured interoperability with other EHRs. The product enabled Athenahealth to open up their APIs for accelerated innovation for their provider base [69]. In January 2018, Apple adopted SMART standards for their Health Kit; others are expected to follow suit. Patients will soon come to expect that their health data be accessed via a range of apps on their phone.

Successful interoperability will rely on widely adopted standardization in data storage and retrieval. Systematized Nomenclature of Medicine-Clinical Terms (SNOMED-CT), Logical Observation Identifiers Names and Codes (LOINC), and RxNorm, a standardizing nomenclature for a medication that can interpret varying vocabulary used by pharmacy and drug interaction software, are increasingly used globally. Health Level 7 (HL7) enables health records and exchanges to be built with typical architecture and structure. Fast Healthcare Interoperability Resources (FHIR), building off HL7 standards, provides data formats and resources for building APIs for facilitating exchange. Project Argonaut, for example, a consortium involving governmental, private and academic health IT leaders, has incorporated these standards to begin work on supporting the uptake of APIs and including them in “meaningful use” regulation [17,70]. India was an early adopter of many of these standards but remains a slow implementer, given the absence of incentives (or penalties) for adoption.

Data Minimization

The architects of India’s digital health infrastructure, while being compliant with global standards, may consider creating a series of “minimum datasets” for standardization and interoperability. In this article, the use of the term *minimum data set* denotes the least possible number of data points that early digital health information systems in India must include to be useful to a range of stakeholders. Obfuscating digitization with validity, new digitized data collection tools are frequently bloated with information that will either not be used or is already being collected elsewhere. A minimal viable product, instead, will help seed the ecosystem and can be incrementally expanded upon, not unlike the phased requirements seen with HITECH. This approach will allow a vast range of pilots to be tested, evaluated, optimized to meet contextually relevant needs, and then scaled up. Data minimization is also a useful tool in improving security and reducing privacy abuse [71]. In India, focusing on *structured* laboratory data, radiology results, medications lists (ie, in sync with interactions at the chemist), allergies, diagnoses, and essential demographic information would provide enough data to spurn a variety of applications for all involved stakeholders.

Substitutability

It is imperative that early prototypes pay critical attention to the user experience. Attempts at EHR adoption in India have failed to date due to the untenable combination of very high patient volume and poor usability. Once again, an API-enabled system will allow providers and institutions to select products that are highly customized to the local context and workflow [72]. Such “substitutability” will be central to advancement—apps that access underlying data that can be updated or swapped out for

new ones with improved features and usability, just as we currently do with apps from an app store [15].

The Law

Traditional privacy principles have been articulated in the Organization for Economic Cooperation and Development guidelines first published in the 1980s, revised last in 2013, the European Directive 95/46/EC, and several pieces of national legislation. These principles have come under increasing scrutiny with the power of big data analytics to combine information from discreet datasets. The EU General Data Protection Regulation (GDPR), considered one of the most stringent of data protection laws came into effect on May 25, 2018. It adopts a rights-based framework, placing the individual at the center of the law. In the United States, while the public sector is mostly governed by the Fair Information Practice Principles and related acts, data flow in the private sector is primarily regulated by notice and consent and overseen mostly by the Federal Trade Commission.

As India’s planners imagine its new technologically powered health data ecosystem, hard questions need to be answered. For example, what risks do we pose for individuals and populations by allowing such seamless data travel? Who owns the data? Can such data be sold? If yes, does the patient have a financial claim, even when data are de-identified? What protection measures need to be put in place? What remedy does the patient have? What legal risks do patients, providers, scientists, and governments expose themselves or each other to? Are the technologies for such secure, encrypted, failsafe ecosystems available? What can we learn from other industries? Why have previous attempts failed?

Emerging economies often lack dedicated privacy laws, relying instead on a patchwork of consumer protection laws, telecommunications statutes, human rights provisions and other measures to tackle data breaches, privacy violations, and constitutionally protected rights to equal treatment. However, as government welfare and benefits are increasingly delivered through online platforms on the backs of newly digitized databases, there is a need to ramp up the legal infrastructure in parallel [73]. This need is critically felt when examining the ability of illiterate users to provide informed consent and to exercise control over valuable data. By engineering interoperable systems that default to protect and empower users by offering them control and discretion over data sharing arrangements, one can optimize the benefits of exchange without compromising privacy or security.

Data mining of de-identified information can now reveal very sensitive data [74-76]. Insurance premiums (in a less regulated health care system), for example, can be modified based on zip codes, browser history or seemingly unrelated shopping habits [75,77]. Technology is not neutral, and most systems encode values and biases, however unconscious [78,79]. Evolving research highlights the risks of data-driven or algorithmic decision-making [80,81]. Biometrics, which systems rely upon for identity verification, has been shown to have higher error rates (false positives and false negatives) for darker skin tones [82].

Societal expectations of privacy can also ebb and flow, and the laws need to be nimble enough to accommodate for the fast pace of IT evolution. Only a few years ago, the idea that Google would scan emails to automatically populate a person's calendar or send alerts was considered highly unacceptable. Today, for many, it is the norm.

In August 2017, the Supreme Court of India ruled that privacy is a fundamental right [83]. The landmark judgment potentially provides the necessary deterrents to data misuse in a health IT ecosystem, in addition to establishing the supremacy of patient's control over her health data (privacy). The Ministry of Electronics and Information Technology constituted an expert committee to help draft a bill on data protection. The committee released a White Paper on the data protection framework for India, inviting public comment [84]. The White Paper extensively examined best practices elsewhere in the world, with particular attention to European Commission's GDPR regulations scheduled to go into effect on May 25, 2018.

Responses to the White Paper included recommendations focused on the protection and use of health data, calling for automated but consented flows, easier access, and portability, and without jeopardizing the safety or privacy of vast swathes of India's digitally illiterate populations. Reviewers opined that health data are generated jointly by the patient and the provider, and are used for purposes beyond clinical care, including for research, operations, payments, quality control, and public health. The patient serves as the "data controller" with a reasonable say in which of their data are made available, to whom, and when. A "data processor" co-creates and adds data to the patient's health record and accesses it when implicitly or explicitly authorized to do so. When patients cannot consent for lack of capacity, illiteracy, or circumstance, regulations should favor the patient's best interest [85]. It might be useful to think about control in the context of a tiered hierarchy of permissions. The patient in most respects would be the final arbiter. Below the patient is a category of stakeholders with access to the data because they have been involved in its creation and to whom the patient has given implicit or explicit consent. Subordinate to these creators of data will be various other actors who can only gain access to the data with the patient's permission or, if permitted by law, without [86].

In March 2018, the MoHFW invited public comment on a new bill it has proposed, the Digital Information Security in Health Care Act [87]. These evolving privacy and data protection laws in India must provide for deterrents to data misuse, where violations result in hefty fines, loss of access, and censure. On the other hand, an onerous, manual, consent-driven process would prevent patients from benefiting from advances in voice-activated services, machine learning, and artificial intelligence. Users of health data must therefore, above all, be expected to have a fiduciary responsibility toward the patient.

Conclusion

In July 2018, the Government of India's NITI Aayog, the National Institute for Transforming India, published a blueprint for a "National Health Stack," embracing the principles of federated patient-centric data flows outlined in this paper

[88,89]. The proposed "Health Stack" platform has the potential for revolutionizing medical care, research, and health care delivery in India. However, a simple, claims-driven model risks replicating the pitfalls of the US system [55]. It is also not likely to inspire provider or patient adoption.

For this proposed technological framework to meet its game-changing potential, the model will benefit from adhering to the following principles: (1) adopting a federated architecture, (2) prioritizing patient and population health needs over billing needs, (3) guaranteeing a patient's right to her structured data, (4) allowing a plug and play model of highly customizable applications that can address varying context-specific needs, and that respond to market incentives for better user-interfaces, (5) mandating minimum data sets, (6) adopting privacy by design: automate audited and consented data flow, and finally (7) defaulting to safeguarding patients' control over their data.

For patients, scientists and clinical providers to recognize, adopt and benefit from the vast potential of a secure, federated health information ecosystem, we propose a suite of initial applications whose benefits to society are palpable. For example, medication alerts, laboratory trends, schedulers and payment logs would prove highly useful to patients but would require interoperability among different sources of data, mandated or incentivized by the state. At a population level, disease surveillance data for modeling and forecasting outbreaks would be particularly useful to public health agencies. Standardized registries for trauma, cancer, rare diseases are desperately needed in India and can be built on the proposed framework. Aggregated and anonymized data sets accessed through an audited trail would help accelerate medical research, given the sheer volume of patient load in India.

However, such widespread adoption and data transfer between entities would necessitate buy-in from multiple stakeholders—through a combination of incentivization, legal mandate, budgetary allocation, and market demand for patient-provider, provider-provider, provider-payer, and payer-patient interactions [22]. There are no PHRs in India. It is precisely the greenfield nature of the digital health ecosystem in India that would allow a PHR-based, API-enabled network from the get-go, pre-empting the development of complex and incompatible silos of health data.

India must take advantage of its vibrant IT ecosystem and the widespread adoption of mobile technologies across its socio-economic strata. A light and robust API-enabled spine upon which both the public and private sector can be invited to build contextually appropriate, competing, substitutable, and incremental solutions will be the key to a forward-looking digital health ecosystem. The time for large centralized data warehouses and homogenous systems has passed.

There is much excitement globally about the power of big data, artificial intelligence and machine learning in reshaping medicine and health care delivery. However, the potential of these promising sciences can only be harnessed with reliable and timely data. A federated PHR in India will provide unprecedented amounts of health data; among them may lie answers to our well-being and happiness.

Acknowledgments

The authors would like to acknowledge the support of the Radcliffe Institute for Advanced Studies at Harvard University for sponsoring the workshop, "Exploring health information exchange: setting an interdisciplinary agenda," in September 2016, where the first draft of this paper was proposed.

Authors' Contributions

SB wrote the first and final drafts of this paper, with significant editorial contributions from AF. All other authors contributed equally.

Conflicts of Interest

None declared.

References

1. Kurian O. The Wire. Why It's a Challenge To Make Quick Sense of India's Health Data URL: <https://thewire.in/health/imr-mmr-data-nss-srs> [accessed 2018-03-25] [WebCite Cache ID 6yBX212wE]
2. Chatterjee P. National Health Protection Scheme revealed in India. *The Lancet* 2018 Feb;391(10120):523-524. [doi: [10.1016/S0140-6736\(18\)30241-1](https://doi.org/10.1016/S0140-6736(18)30241-1)]
3. McGraw D, Dempsey JX, Harris L, Goldman J. Privacy as an enabler, not an impediment: building trust into health information exchange. *Health Aff (Millwood)* 2009;28(2):416-427 [FREE Full text] [doi: [10.1377/hlthaff.28.2.416](https://doi.org/10.1377/hlthaff.28.2.416)] [Medline: [19275998](https://pubmed.ncbi.nlm.nih.gov/19275998/)]
4. Roehrs A, da Costa CA, da Rosa Righi R, de Oliveira KSF. Personal Health Records: A Systematic Literature Review. *J Med Internet Res* 2017 Jan 06;19(1):e13 [FREE Full text] [doi: [10.2196/jmir.5876](https://doi.org/10.2196/jmir.5876)] [Medline: [28062391](https://pubmed.ncbi.nlm.nih.gov/28062391/)]
5. Perlin JB. Health Information Technology Interoperability and Use for Better Care and Evidence. *JAMA* 2016 Oct 25;316(16):1667-1668. [doi: [10.1001/jama.2016.12337](https://doi.org/10.1001/jama.2016.12337)] [Medline: [27669026](https://pubmed.ncbi.nlm.nih.gov/27669026/)]
6. Tang PC, Lansky D. The missing link: bridging the patient-provider health information gap. *Health Aff (Millwood)* 2005;24(5):1290-1295 [FREE Full text] [doi: [10.1377/hlthaff.24.5.1290](https://doi.org/10.1377/hlthaff.24.5.1290)] [Medline: [16162575](https://pubmed.ncbi.nlm.nih.gov/16162575/)]
7. Tang PC, Ash JS, Bates DW, Overhage JM, Sands DZ. Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. *J Am Med Inform Assoc* 2006;13(2):121-126 [FREE Full text] [doi: [10.1197/jamia.M2025](https://doi.org/10.1197/jamia.M2025)] [Medline: [16357345](https://pubmed.ncbi.nlm.nih.gov/16357345/)]
8. Steele R, Min K, Lo A. Personal health record architectures: Technology infrastructure implications and dependencies. *Acta Anaesthesiol Scand* 2012 Mar 05;63(6):1079-1091. [doi: [10.1002/asi.22635](https://doi.org/10.1002/asi.22635)]
9. Archer N, Fevrier-Thomas U, Lokker C, McKibbin KA, Straus SE. Personal health records: a scoping review. *J Am Med Inform Assoc* 2011;18(4):515-522 [FREE Full text] [doi: [10.1136/amiajnl-2011-000105](https://doi.org/10.1136/amiajnl-2011-000105)] [Medline: [21672914](https://pubmed.ncbi.nlm.nih.gov/21672914/)]
10. Baird A, North F, Raghu T. Personal Health Records (PHR) and the future of the physician-patient relationship. : ACM International Conference Proceeding Series; 2011 Presented at: iConference 2011; Feb 8-11, 2011; Seattle, WA, USA p. 281-288. [doi: [10.1145/1940761.1940800](https://doi.org/10.1145/1940761.1940800)]
11. Spil T, Klein R. The personal health future. *Health Policy and Technology* 2015 Jun;4(2):131-136. [doi: [10.1016/j.hlpt.2015.02.004](https://doi.org/10.1016/j.hlpt.2015.02.004)]
12. Pushpangadan S, Seckman C. Consumer perspective on personal health records: A review of the literature. *Online Journal of Nursing Informatics* 2015 Feb 04;19(1):A [FREE Full text]
13. My Health Record. Personal Health Record Locker URL: <https://myhealthrecord.nhp.gov.in/> [accessed 2018-03-25] [WebCite Cache ID 6yBdYdYLL]
14. Research2Guidance. 2016. mHealth App Developer Economics 2016 URL: <https://research2guidance.com/r2g/r2g-mHealth-App-Developer-Economics-2016.pdf> [accessed 2018-03-25] [WebCite Cache ID 6yBdtUZ4Y]
15. Mandl KD, Kohane IS. A 21st-Century Health IT System - Creating a Real-World Information Economy. *N Engl J Med* 2017 May 18;376(20):1905-1907. [doi: [10.1056/NEJMp1700235](https://doi.org/10.1056/NEJMp1700235)] [Medline: [28514623](https://pubmed.ncbi.nlm.nih.gov/28514623/)]
16. PwC. India: PricewaterhouseCooper Private Ltd; 2017. How mHealth can revolutionise the Indian healthcare industry URL: <https://www.pwc.in/assets/pdfs/publications/2017/how-mhealth-can-revolutionise-the-indian-healthcare-industry.pdf> [accessed 2018-06-10] [WebCite Cache ID 6zLhayWH9]
17. Mandl KD, Mandel JC, Kohane IS. Driving Innovation in Health Systems through an Apps-Based Information Economy. *Cell Syst* 2015 Jul;1(1):8-13 [FREE Full text] [doi: [10.1016/j.cels.2015.05.001](https://doi.org/10.1016/j.cels.2015.05.001)] [Medline: [26339683](https://pubmed.ncbi.nlm.nih.gov/26339683/)]
18. Russel J. India's Practo raises \$55M to expand its healthcare platform to more emerging markets. 2017 Jan 17. Tech Crunch URL: <https://techcrunch.com/2017/01/16/practo-raises-55-million-series-d-led-by-tencent/> [WebCite Cache ID 6zLjMYq6S]
19. Baldwin JL, Singh H, Sittig DF, Giardina TD. Patient portals and health apps: Pitfalls, promises, and what one might learn from the other. *Healthc (Amst)* 2016 Oct 3:81-85 [FREE Full text] [doi: [10.1016/j.hjdsi.2016.08.004](https://doi.org/10.1016/j.hjdsi.2016.08.004)] [Medline: [27720139](https://pubmed.ncbi.nlm.nih.gov/27720139/)]

20. Bedoya A. Comments of Alvaro Bedoya, Center on Privacy & Technology at Georgetown Law, on.: Georgetown Law Aug 15, 2014 URL: https://www.ftc.gov/system/files/documents/public_comments/2014/08/00024-92434.pdf [WebCite Cache ID 6zLkCHpVW]
21. Powles J, Hodson H. Google DeepMind and healthcare in an age of algorithms. *Health Technol (Berl)* 2017;7(4):351-367 [FREE Full text] [doi: [10.1007/s12553-017-0179-1](https://doi.org/10.1007/s12553-017-0179-1)] [Medline: [29308344](https://pubmed.ncbi.nlm.nih.gov/29308344/)]
22. Halamka JD, Tripathi M. The HITECH Era in Retrospect. *N Engl J Med* 2017 Sep 07;377(10):907-909. [doi: [10.1056/NEJMp1709851](https://doi.org/10.1056/NEJMp1709851)] [Medline: [28877012](https://pubmed.ncbi.nlm.nih.gov/28877012/)]
23. Woods SS, Schwartz E, Tuepker A, Press NA, Nazi KM, Turvey CL, et al. Patient experiences with full electronic access to health records and clinical notes through the My HealthVet Personal Health Record Pilot: qualitative study. *J Med Internet Res* 2013;15(3):e65 [FREE Full text] [doi: [10.2196/jmir.2356](https://doi.org/10.2196/jmir.2356)] [Medline: [23535584](https://pubmed.ncbi.nlm.nih.gov/23535584/)]
24. Ballantyne A, Schaefer GO. Consent and the ethical duty to participate in health data research. *J Med Ethics* 2018 Jun;44(6):392-396. [doi: [10.1136/medethics-2017-104550](https://doi.org/10.1136/medethics-2017-104550)] [Medline: [29358219](https://pubmed.ncbi.nlm.nih.gov/29358219/)]
25. White J, Briggs J, Mandel J. NIH and ONC Launch the Sync for Science (S4S) Pilot Enabling Individual Health Data Access and Donation. 2016 URL: <https://www.healthit.gov/buzz-blog/health-innovation/nih-and-onc-launch-the-sync-for-science-pilot/> [accessed 2018-03-25] [WebCite Cache ID 6yBfHcOrC]
26. Mohanan M, Hay K, Mor N. Quality Of Health Care In India: Challenges, Priorities, And The Road Ahead. *Health Aff (Millwood)* 2016 Dec 01;35(10):1753-1758. [doi: [10.1377/hlthaff.2016.0676](https://doi.org/10.1377/hlthaff.2016.0676)] [Medline: [27702945](https://pubmed.ncbi.nlm.nih.gov/27702945/)]
27. Basu S, Andrews J, Kishore S, Panjabi R, Stuckler D. Comparative performance of private and public healthcare systems in low- and middle-income countries: a systematic review. *PLoS Med* 2012;9(6):e1001244 [FREE Full text] [doi: [10.1371/journal.pmed.1001244](https://doi.org/10.1371/journal.pmed.1001244)] [Medline: [22723748](https://pubmed.ncbi.nlm.nih.gov/22723748/)]
28. Anand S, Fan V. The Health Workforce in India: Human Resources for Health Observer Series No. 2016 URL: http://www.who.int/hrh/resources/16058health_workforce_India.pdf [accessed 2018-03-25] [WebCite Cache ID 6yBfugwBk]
29. Central Bureau of Health Intelligence, Ministry of Health and Family Welfare. National Health Profile 2017 URL: http://www.indiaenvironmentportal.org.in/files/file/NHP_2017-1.pdf [accessed 2018-05-20] [WebCite Cache ID 6zZBDDuAP]
30. Balsari S, Simon G, Nair R, Saunik S, Phadke M. Task shifting in health care: the risks of integrated medicine in India. *Lancet Glob Health* 2017 Dec;5(10):e963-e964 [FREE Full text] [doi: [10.1016/S2214-109X\(17\)30322-4](https://doi.org/10.1016/S2214-109X(17)30322-4)] [Medline: [28911757](https://pubmed.ncbi.nlm.nih.gov/28911757/)]
31. Srivastava SK. Adoption of Electronic Health Records: A Roadmap for India. *Healthc Inform Res* 2016 Oct;22(4):261-269 [FREE Full text] [doi: [10.4258/hir.2016.22.4.261](https://doi.org/10.4258/hir.2016.22.4.261)] [Medline: [27895957](https://pubmed.ncbi.nlm.nih.gov/27895957/)]
32. Sharma M, Aggarwal H. HER Adoption in India: Potential and the Challenges. *Indian Journal of Science and Technology Sep* 2016;9(34):1-7.
33. HiMMS Analytics. Stage 6 Hospitals URL: <http://www.himssanalyticsasia.org/emram/stage6hospitals.asp> [accessed 2018-05-12] [WebCite Cache ID 6zMsQhnc3]
34. Powell AC, Ludhar JK, Ostrovsky Y. Electronic health record use in an affluent region in India: Findings from a survey of Chandigarh hospitals. *Int J Med Inform* 2017 Dec;103:78-82. [doi: [10.1016/j.ijmedinf.2017.04.011](https://doi.org/10.1016/j.ijmedinf.2017.04.011)] [Medline: [28551005](https://pubmed.ncbi.nlm.nih.gov/28551005/)]
35. Patel V, Parikh R, Nandraj S, Balasubramaniam P, Narayan K, Paul VK, et al. Assuring health coverage for all in India. *Lancet* 2015 Dec 12;386(10011):2422-2435. [doi: [10.1016/S0140-6736\(15\)00955-1](https://doi.org/10.1016/S0140-6736(15)00955-1)] [Medline: [26700532](https://pubmed.ncbi.nlm.nih.gov/26700532/)]
36. Growth Analysis. Östersund, Sweden: Swedish Agency for Growth Policy Analysis; 2013 Apr. India's Healthcare System: Overview and Quality Improvements URL: http://www.tillvaxtanalys.se/download/18.5d9caa4d14d0347533bcf42e/1430909773826/direct_response_2013_04.pdf [WebCite Cache ID 6yC3wjnu7]
37. Vital Wave Consulting. 2009 May. Health Information Systems in Developing Countries URL: <http://www.minsa.gob.pe/oge/conferenciaops/Recursos/43.pdf> [WebCite Cache ID 6yC4EncMb]
38. eMaharashtra. Healthcare & Academics Management & Information System URL: <https://bit.ly/2zsRg0e> [WebCite Cache ID 6yC5Nc1uu]
39. Natarajan S, Panchanathan V, Bansal PK. Health Management Information System Implemented in Government Hospitals of Tamil Nadu. *International Journal of Scientific and Engineering Research* 2013 Oct;4(10):282-288 [FREE Full text]
40. Amrita Technologies. A sample of Clients using Amrita HIS URL: <http://www.amritatech.com/customers.html> [accessed 2018-05-12] [WebCite Cache ID 6zN0OCYCg]
41. Gujarat Medical Services Corporation Limited. E-Aushadhi URL: <https://gmscl.gujarat.gov.in/e-aushadhi-eng.htm> [accessed 2018-05-12] [WebCite Cache ID 6zMuyNck4]
42. E-Aushadhi. Rajasthan Medical Services Corporation Ltd. e-Aushadhi URL: <http://e-aushadhi.rajasthan.gov.in/DWH/startup/loginAction> [accessed 2018-05-12] [WebCite Cache ID 6zN0kfvJT]
43. Ministry of Health and Family Welfare, Government of India. 2013 Apr. Recommendations On Electronic Medical Records Standards In India URL: <https://mohfw.gov.in/sites/default/files/24539108839988920051EHR%20Standards-v5%20Apr%202013.pdf> [accessed 2018-03-25] [WebCite Cache ID 6yC4mI90b]
44. Rustagi N, Singh R. Electronic medical record: Time to migrate? *Perspect Clin Res* 2012 Oct;3(4):143-145 [FREE Full text] [doi: [10.4103/2229-3485.103596](https://doi.org/10.4103/2229-3485.103596)] [Medline: [23293762](https://pubmed.ncbi.nlm.nih.gov/23293762/)]
45. Dandona L, Sivan YS, Jyothi MN, Bhaskar VSU, Dandona R. The lack of public health research output from India. *BMC Public Health* 2004 Nov 25;4:55 [FREE Full text] [doi: [10.1186/1471-2458-4-55](https://doi.org/10.1186/1471-2458-4-55)] [Medline: [15563377](https://pubmed.ncbi.nlm.nih.gov/15563377/)]

46. Shah J, Pawaskar A, Kumar S, Kshirsagar N. Outcomes research resources in India: current status, need and way forward. Springerplus 2013;2:518 [FREE Full text] [doi: [10.1186/2193-1801-2-518](https://doi.org/10.1186/2193-1801-2-518)] [Medline: [24171151](https://pubmed.ncbi.nlm.nih.gov/24171151/)]
47. Jain D. LiveMint. 2018 Jan 25. Budget 2018: India's health sector needs more funds and better management URL: <https://www.livemint.com/Politics/drnszDrkbt418WpuQEhfZI/Budget-2018-Indias-health-sector-needs-more-funds-and-bett.html> [accessed 2018-03-26] [WebCite Cache ID [6yC61SwYi](https://www.webcitation.org/6yC61SwYi)]
48. SNOMED International India. URL: <https://www.snomed.org/member/india> [accessed 2018-03-26] [WebCite Cache ID [6yC6c3a2b](https://www.webcitation.org/6yC6c3a2b)]
49. Adler-Milstein J, Jha A. HITECH Act Drove Large Gains In Hospital Electronic Health Record Adoption. Health Aff (Millwood) 2017 Aug 01;36(8):1416-1422. [doi: [10.1377/hlthaff.2016.1651](https://doi.org/10.1377/hlthaff.2016.1651)] [Medline: [28784734](https://pubmed.ncbi.nlm.nih.gov/28784734/)]
50. Blumenthal D, Tavenner M. The "meaningful use" regulation for electronic health records. N Engl J Med 2010 Aug 05;363(6):501-504. [doi: [10.1056/NEJMp1006114](https://doi.org/10.1056/NEJMp1006114)] [Medline: [20647183](https://pubmed.ncbi.nlm.nih.gov/20647183/)]
51. Ministry of Health & Family Welfare, Government of India. 2017 Oct. National Health Accounts Estimates for India 2014-2015 URL: <https://mohfw.gov.in/sites/default/files/National%20Health%20Accounts%20Estimates%20Report%202014-15.pdf> [accessed 2018-03-25] [WebCite Cache ID [6yC7EfdLp](https://www.webcitation.org/6yC7EfdLp)]
52. Mandl KD, Kohane IS. Escaping the EHR trap--the future of health IT. N Engl J Med 2012 Jun 14;366(24):2240-2242. [doi: [10.1056/NEJMp1203102](https://doi.org/10.1056/NEJMp1203102)] [Medline: [22693995](https://pubmed.ncbi.nlm.nih.gov/22693995/)]
53. Ministry of Health and Family Welfare, Government of India. 2016 Dec. Electronic Health Record (EHR) Standards for India URL: <https://www.nhp.gov.in/NHPfiles/EHR-Standards-2016-MoHFW.pdf> [accessed 2018-03-25] [WebCite Cache ID [6yC7bionK](https://www.webcitation.org/6yC7bionK)]
54. Ministry of Health and Family Welfare.: Government of India National Health Policy, 2017 URL: https://www.nhp.gov.in/NHPfiles/national_health_policy_2017.pdf [accessed 2018-03-26] [WebCite Cache ID [6yC821ZLM](https://www.webcitation.org/6yC821ZLM)]
55. Kandhari R. The Ken. 2018 Jan 08. India picks a builder for its health data hub URL: <https://the-ken.com/story/ihp-health-data-hub/> [accessed 2018-03-26] [WebCite Cache ID [6yC8sExDv](https://www.webcitation.org/6yC8sExDv)]
56. Mandl KD, Kohane IS. Time for a Patient-Driven Health Information Economy? N Engl J Med 2016 Jan 21;374(3):205-208 [FREE Full text] [doi: [10.1056/NEJMp1512142](https://doi.org/10.1056/NEJMp1512142)] [Medline: [26789868](https://pubmed.ncbi.nlm.nih.gov/26789868/)]
57. Iansiti M, Lakhani K. Harvard Business Review. 2017. The Truth About Blockchain URL: <https://hbr.org/2017/01/the-truth-about-blockchain> [accessed 2018-03-26] [WebCite Cache ID [6yCGq7zQP](https://www.webcitation.org/6yCGq7zQP)]
58. Peterson K, Deeduvanu R, Kanjamala P, Boles K. healthIT. 2016. A Blockchain-Based Approach to Health Information Exchange Networks URL: <https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf> [WebCite Cache ID [6zMwHIFuX](https://www.webcitation.org/6zMwHIFuX)]
59. Fomkin R, Stenbeck M, Litton J. Federated Databases as a Basis for Infrastructure Supporting Epidemiological Research. 2009 Sep 03 Presented at: 20th International Workshop on Database and Expert Systems Application; 2009; Linz, Austria p. 313-317. [doi: [10.1109/DEXA.2009.56](https://doi.org/10.1109/DEXA.2009.56)]
60. Statista. Share of mobile phone users that use a smartphone in India from 2014 to 2019 URL: <https://www.statista.com/statistics/257048/smartphone-user-penetration-in-india/> [accessed 2018-03-26] [WebCite Cache ID [6zMwqrPsF](https://www.webcitation.org/6zMwqrPsF)]
61. Bhuyan A. The Wire. 2018 Jan 18. Aadhaar Isn't Just About Privacy. There Are 30 Challenges the Govt Is Facing in Supreme Court URL: <https://thewire.in/215017/aadhaar-privacy-government-supreme-court/> [WebCite Cache ID [6yCHbeC5s](https://www.webcitation.org/6yCHbeC5s)]
62. Marcoli C. IBM. 2017 Jul 20. Open banking APIs are open for business URL: <https://www.ibm.com/blogs/insights-on-business/banking/open-banking-apis-are-open-for-business/> [accessed 2018-03-26] [WebCite Cache ID [6yCCQUAvu](https://www.webcitation.org/6yCCQUAvu)]
63. Brodsky L, Oakes L. McKinsey & Company. 2017 Sep. Data sharing and open banking URL: <https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking> [accessed 2018-03-26] [WebCite Cache ID [6yCCffgbb](https://www.webcitation.org/6yCCffgbb)]
64. IndiaStack. What is IndiaStack? URL: <http://indiastack.org/about/> [accessed 2018-03-30] [WebCite Cache ID [6yJH4PSGO](https://www.webcitation.org/6yJH4PSGO)]
65. Unique Identification Authority of India, Government of India. eKYC Dashboard URL: https://uidai.gov.in/aadhaar_dashboard/ekyc_trend.php [accessed 2018-03-26] [WebCite Cache ID [6yCFXpthx](https://www.webcitation.org/6yCFXpthx)]
66. DigiLocker. National eGovernance Division, Ministry of Electronics & Information Technology (MeitY), Government of India URL: <https://digilocker.gov.in/> [accessed 2018-03-26] [WebCite Cache ID [6yCFyKp79](https://www.webcitation.org/6yCFyKp79)]
67. OpenMRS. URL: <https://wiki.openmrs.org/> [accessed 2018-03-25] [WebCite Cache ID [6yCGGzPE7](https://www.webcitation.org/6yCGGzPE7)]
68. SMART. An App Platform for Healthcare URL: <https://smarthealthit.org/> [accessed 2018-03-26] [WebCite Cache ID [6yCGZeFa0](https://www.webcitation.org/6yCGZeFa0)]
69. Bartlett J. Boston Business Journal. 2017 Jun 08. Athenahealth buys Palo Alto software firm for \$63M URL: <https://www.bizjournals.com/boston/news/2017/06/08/athenahealth-buys-palo-alto-software-firm-for-63m.html> [accessed 2018-03-25] [WebCite Cache ID [6yJEm7avE](https://www.webcitation.org/6yJEm7avE)]
70. Halamka J. Life as a Healthcare CIO. 2017 Dec 17. The Argonaut Project Charter URL: <http://geekdoctor.blogspot.com/2014/12/the-argonaut-project-charter.html> [WebCite Cache ID [6yCH27cpZ](https://www.webcitation.org/6yCH27cpZ)]

71. Ross R. Managing Security Privacy Risk in Healthcare Applications. 2012 Presented at: 5th Annual OCR/NIST HIPAA Security Rule Conference; June 6, 2012; Washington, DC URL: https://csrc.nist.gov/CSRC/media/Presentations/Managing-Security-and-Privacy-Risk-in-Healthcare-A/images-media/day1-1_ross_risk-management-controls.pdf
72. Mandl KD, Kohane IS. No small change for the health information economy. *N Engl J Med* 2009 Mar 26;360(13):1278-1281. [doi: [10.1056/NEJMp0900411](https://doi.org/10.1056/NEJMp0900411)] [Medline: [19321867](https://pubmed.ncbi.nlm.nih.gov/19321867/)]
73. Rothstein MA. Is deidentification sufficient to protect health privacy in research? *Am J Bioeth* 2010 Sep;10(9):3-11 [FREE Full text] [doi: [10.1080/15265161.2010.494215](https://doi.org/10.1080/15265161.2010.494215)] [Medline: [20818545](https://pubmed.ncbi.nlm.nih.gov/20818545/)]
74. Rothstein MA. Is deidentification sufficient to protect health privacy in research? *Am J Bioeth* 2010 Sep;10(9):3-11 [FREE Full text] [doi: [10.1080/15265161.2010.494215](https://doi.org/10.1080/15265161.2010.494215)] [Medline: [20818545](https://pubmed.ncbi.nlm.nih.gov/20818545/)]
75. de Montjoye YA, Hidalgo CA, Verleysen M, Blondel VD. Unique in the Crowd: The privacy bounds of human mobility. *Sci Rep* 2013;3:1376 [FREE Full text] [doi: [10.1038/srep01376](https://doi.org/10.1038/srep01376)] [Medline: [23524645](https://pubmed.ncbi.nlm.nih.gov/23524645/)]
76. Brickell J, Shmatikov V. The Cost of Privacy: Destruction of Data-Mining Utility in Anonymized Data Publishing. 2008 Aug Presented at: Proceeding of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining - KDD 08; 2008; Las Vegas, Nevada p. 70-78.
77. de Montjoye YA, Radaelli L, Singh VK, Pentland AS. Identity and privacy. Unique in the shopping mall: on the reidentifiability of credit card metadata. *Science* 2015 Jan 30;347(6221):536-539. [doi: [10.1126/science.1256297](https://doi.org/10.1126/science.1256297)] [Medline: [25635097](https://pubmed.ncbi.nlm.nih.gov/25635097/)]
78. Young L. IEEE Spectrum. Computer Scientists Find Bias in Algorithms URL: <https://spectrum.ieee.org/tech-talk/computing/software/computer-scientists-find-bias-in-algorithms> [accessed 2018-03-26] [WebCite Cache ID 6yCIeryis]
79. Simonite T. MIT Technology Review. 2015 Jul 06. Probing the Dark Side of Google's Ad-Targeting System URL: <https://www.technologyreview.com/s/539021/probing-the-dark-side-of-googles-ad-targeting-system/> [WebCite Cache ID 6yJF2siVy]
80. Sweeney L. Discrimination in online ad delivery. *Commun. ACM* 2013 May 01;56(5):44. [doi: [10.1145/2447976.2447990](https://doi.org/10.1145/2447976.2447990)]
81. Kirchner L. The Atlantic. 2015 Jul 06. When Discrimination Is Baked Into Algorithms URL: <https://www.theatlantic.com/business/archive/2015/09/discrimination-algorithms-disparate-impact/403969/> [accessed 2018-03-25] [WebCite Cache ID 6yCJXkcfj]
82. Buolamwini J, Gebru T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research* 2018:1-15.
83. Supreme Court of India Civil Original Jurisdiction. Writ Petition (Civil) No 494 of 2012 URL: http://supremecourtindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf [accessed 2018-03-26] [WebCite Cache ID 6yDTIjUpp]
84. Ministry of Electronics and Information Technology, Government of India. 2018. White Paper on Data Protection framework for India URL: <http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited> [accessed 2018-03-25] [WebCite Cache ID 6yDTYvald]
85. Harvard FXB Center for Health and Human Rights. 2018 Feb 08. Harvard FXB Responds to White Paper on Data Protection Framework for India URL: <https://fxb.harvard.edu/2018/02/08/harvard-fxb-responds-to-white-paper-on-data-protection-framework-for-india/> [accessed 2018-03-25] [WebCite Cache ID 6yCI3xOKB]
86. Balsari S, Babha J. Jan 31. 2018. Responses to the White Paper of the Committee of Experts on Data Protection Framework for India URL: <https://cdn2.sph.harvard.edu/wp-content/uploads/sites/5/2018/02/RHarvard-FXB-Responses-to-WP-Health-Data-FINAL.pdf> [accessed 2018-03-26] [WebCite Cache ID 6yDTzD1r9]
87. Ministry of Health & Family Welfare, Government of India. 2017 Nov. Digital Information Security in Healthcare, Act URL: https://mohfw.gov.in/sites/default/files/R_4179_1521627488625_0.pdf [accessed 2018-03-21] [WebCite Cache ID 6yDUMIarO]
88. Press Information Bureau, Government of India. Comments Invited for Creation of National Health Stack. 2018 Jul 06. URL: <http://pib.nic.in/PressReleaseDetail.aspx?PRID=1538061>
89. Government of India, NITI Aayog. National Health Stack: Strategy and Approach. 2018 Jul. URL: http://www.niti.gov.in/writereaddata/files/document_publication/NHS-Strategy-and-Approach-Documents-for-consultation.pdf

Abbreviations

- API:** application programming interface
- EHR:** electronic health record
- FHIR:** Fast Healthcare Interoperability Resources
- GDPR:** General Data Protection Regulation
- HIE:** Health Information Exchange
- HITECH:** Information Technology for Economic and Clinical Health
- ID:** identification
- IHIP:** Integrated Health Information Platform
- IT:** information technology

KYC: know your customer

LOINC: Logical Observation Identifiers Names and Codes

MoHFW: The Ministry of Health and Family Welfare

NHPS: National Health Protection Scheme

PHR: personal health record

SNOMED-CT: Systematized Nomenclature of Medicine-Clinical Terms

Edited by G Eysenbach; submitted 07.04.18; peer-reviewed by R Chandrasekaran, D Walker, P Yao, I Adeleke; comments to author 02.05.18; revised version received 25.05.18; accepted 09.06.18; published 13.07.18

Please cite as:

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

J Med Internet Res 2018;20(7):e10725

URL: <http://www.jmir.org/2018/7/e10725/>

doi: [10.2196/10725](https://doi.org/10.2196/10725)

PMID: [30006325](https://pubmed.ncbi.nlm.nih.gov/30006325/)

©Satchit Balsari, Alexander Fortenko, Joaquín A. Blaya, Adrian Gropper, Malavika Jayaram, Rahul Matthan, Ram Sahasranam, Mark Shankar, Suptendra N Sarbadhikari, Barbara E Bierer, Kenneth D Mandl, Sanjay Mehendale, Tarun Khanna. Originally published in the Journal of Medical Internet Research (<http://www.jmir.org>), 13.07.2018. This is an open-access article distributed under the terms of the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work, first published in the Journal of Medical Internet Research, is properly cited. The complete bibliographic information, a link to the original publication on <http://www.jmir.org/>, as well as this copyright and license information must be included.