Rebooting consent in the digital age: a governance framework for health data exchange

Proposed Title:

Rebooting Consent in the Digital Age: A Governance Framework for Health Data Exchange

Corresponding Author:
Satchit Balsari, MD, MPH
FXB Center for Health and Human Rights
Harvard TH Chan School of Public Health
651 Huntington Avenue, 703C
Boston, MA, United States
Phone: 1 6174951000
Email: balsari@hsph.harvard.edu

Authors:
Nivedita Saksena,[1,2] Rahul Matthan,[3,4] Anant Bhan,[5] Satchit Balsari[2,6]

[1]The Lakshmi Mittal and Family South Asia Institute, Harvard University, Cambridge, MA, United States
[2]FXB Center for Health and Human Rights, Harvard TH Chan School of Public Health, Boston, MA, United States
[3]The Takshashila Institution, Bengaluru, India
[4]Trilegal, Bengaluru, India
[5]Global Health, Bioethics & Health Policy, Bhopal, India
[6]Department of Emergency Medicine, Beth Israel Deaconess Medical Center and Harvard Medical School, Boston, MA, United States

Competing Interests:
NS and SB report grants from Tata Trusts and Dell Giving outside the submitted work.

Word Count: 3056

ABSTRACT

In August 2020, India announced its vision for the National Digital Health Mission (NDHM), a federated national digital health exchange where digitised data generated by healthcare providers will be exported via Application Program Interfaces to the patient's electronic personal health record. The NDHM architecture is initially expected to be a claims platform for the national health insurance program 'Ayushman Bharat' that serves 500 million people. Such large-scale digitisation and mobility of health data will have significant ramifications on care delivery, population health planning, as well as on the rights and privacy of individuals. Traditional mechanisms that seek to protect individual autonomy through patient consent will be inadequate in a digitised ecosystem where processed data can travel near instantaneously across various nodes in the system and be combined, aggregated, or even re-identified.

In this paper we explore the limitations of 'informed' consent that is sought either when data are collected or when they are ported across the system. We examine the merits and limitations of proposed alternatives like the fiduciary framework that imposes accountability on those that use the data; privacy by design principles that rely on technological safeguards against abuse; or regulations. Our recommendations combine complementary approaches in light of the evolving jurisprudence in India and provide a generalisable framework for health data exchange that balances individual rights with advances in data science.

Summary Box:

- Traditional mechanisms that seek to protect individual autonomy through patient consent are inadequate in a digitised ecosystem.
- It is impossible to truly foresee how data may be combined and recombined and eventually used, making rational choices about future use of data uninformed, if not ineffective.
- We examine the merits and limitations of proposed alternatives like the fiduciary obligations that hold data processors accountable; privacy by design principles that rely on technological safeguards against abuse; and regulatory frameworks.
- We favour the creation of an enabling regulatory environment where PbD principles can be leveraged not only to allow safe data exchange, but also to embed enforceability at scale.
- Our recommendations combine complementary approaches in light of the evolving jurisprudence in India and provide a generalisable framework for health data exchange that balances individual rights with advances in data science.

INTRODUCTION

The COVID-19 pandemic has underscored the need for a robust digital health ecosystem to deliver telemedicine,[1,2] remote care[3,4] and supervised task-shifting.[5,6] In India, the urgent need to compensate providers for COVID-19 care through the national health insurance scheme, Ayushman Bharat, accelerated the institution of a federated digital health ecosystem, the National Digital Health Mission (NDHM).[7] Borrowing heavily from technological innovations in the financial sector, the NDHM seeks to use a 'consent manager' to regulate data exchange between patients, provider, payers and others. The volume of daily data transactions expected across this ecosystem servicing 1.3 billion people raises significant privacy concerns.

Health data have typically been protected through consent, de-identification, and ring fencing of storage and access.[8] Advances in data science however render these traditional approaches ineffective, making it possible to re-identify individuals or groups with relative ease.[9,10] This article begins by describing the use and limits of consent in contemporary clinical practice and research, followed by an examination of three proposed alternatives: a) the placing of fiduciary obligations on data processors; b) privacy by design; and c) and expanding regulation. We call for a complementary, contextually intelligent approach that balances the need for privacy with the opportunity to responsibly use data to advance medicine and public health.

1. CONSENT AND ITS LIMITATIONS

Informed consent is a key tenet in medicine, and is often understood as the explicit documented approval given by a patient to receive medical interventions after having reflected on related benefits and harms.[11] The seeking of consent to collect and use patients' data including from their medical records, radiological images and tissue samples is, however, less explicit.

Coercion and Obfuscation

In most primary care settings in India, general practitioners seldom maintain any records, and consent is not sought when they do. Community health workers however routinely collect large volumes of data, but also without explicit consent or explanation about how the data will be used .[12] In modern hospitals, if consent is sought for the collection or use of data, it is documented during patient registration, or often at the bedside just prior to interventions. The power hierarchy operating in such interactions impedes true autonomous decision making and is particularly exacerbated when services are sought by individuals already discriminated against by literacy, gender, caste, or class. Such rule-based consent for data collection satisfies formal legal requirements but is coercive[13] and does not constitute what Faden and Beauchamp[14] described as true 'autonomous authorisation'.

Routinisation of consent

Health data are also increasingly exchanged across services such as wearables, apps and some point-of-care devices that are governed by weak data protection regulations. The language, length and complexity of consent documents[15,16] accessed through small screens on mobile devices or wearables with little or no true choices have rendered them irrelevant, opaque, non-comparable and inflexible.[17] Long privacy policy notices result in “consent fatigue” and exacerbate the “routinisation” of consent, where its provision merely signals compliance to gain access, and it is not longer informed or meaningful.[18]

Attempts to address the challenges with consent for collecting data (collection consent) have included dynamic consent, shorter consent forms, and multimedia aids, all with limited success.[19] Consent for exchanging or transmitting collected data (portability consent) has been addressed either by a) de-identifying or anonymising data sets rendering the data “non-personal,” and outside of the purview of most privacy protection regulations, or b) seeking ‘blanket’ consent for any use, or ‘broad’ consent for any reasonably foreseeable secondary use of data.[8] We discuss the limits of both approaches below.

A: Side-stepping consent

Large anonymised aggregated human mobility datasets collated from social medial platforms and AdTech companies were used during the COVID-19 pandemic to estimate the impact of social distancing directives.[20,21] Social media users who consented to the secondary use of their data could not have foreseen their use for pandemic response planning. Ethics committees have allowed such use of data because they are no longer ‘identifiable,’ and because the research is in the interest of public good in the midst of an emergency. However, such data when combined with other datasets may violate individual or group privacy through inadvertent or intentional re-identification or inferences.[9,10,22]

It is impossible to truly foresee how geolocation data collected from cell phone towers or AdTech companies, or digital phenotypes (unique characteristics) deduced from health and lifestyle apps may be combined and recombined, making rational choices about future use of data uninformed, if not ineffective.[23,24] Nissenbaum, while noting the ever changing nature of data flow and the cognitive challenges it poses, concludes: "Even if, for a given moment, a snapshot of the information flows could be grasped, the realm is in constant flux, with new firms entering the picture, new analytics, and new backend contracts forged: in other words, we are dealing with a recursive capacity that is indefinitely extensible.”[25]

Downstream commercialisation of data also raises important questions about claims to profits. Consider, for example, a successful machine learning algorithm that has trained on a trove of archived roentgenograms from rural public hospitals and can now accurately detect cancers long before the expert radiologist’s eye. The invention is sold by the start-up for a large amount of

money. The original set of patients may be uncontactable or deceased, while their data are being monetised by a third-party in ways that may have been inconceivable at the time the X-rays were administered. What does the company profiting from their data owe them, if anything at all?

B: Broad and blanket consent

For health data exchanged among laboratories, pharmacies and physicians in the routine care or billing of patients, consent for secondary use is "broad," and in India almost always implicit. The European Union's General Data Protection Regulations (GDPR)[26] and India's Personal Data Protection Bill 2019 (PDP Bill)[27] currently tabled in the Indian parliament, however, prohibit organisations from asking for blanket consent. Organisations cannot make the provision of services dependent on consent to unrelated processing (i.e., cannot ask data principals to "pay" with their data) and cannot treat users' failure to opt out of pre-set settings as implying consent. This makes obtaining consent for processing that does not provide direct, tangible benefits to the data principal difficult even for companies that have direct relationships with end users. Industry advocates have argued that consent-heavy systems thwart innovation, precluding society from benefiting from the application of artificial intelligence and machine learning in the fields of medicine and public health. Users are less likely to consent to processing that offers them little in return or bother to opt into settings they are opted-out of by default, running the potential risk of inadvertently blocking the development of products and technologies that may generate public good.[28] Subsequent sections examine alternative approaches that seek to address these limitations.

2. DATA FIDUCIARIES

The consent-model places the onus of privacy on the data principal – the person whose data is being processed, absolving data processors from using the data responsibly. In the absence of laws, companies such as Amazon,[29,30] Microsoft[31] and Google[32,33] have published voluntary standards on fairness and ethics, largely focus on purging bias from AI algorithms, among growing alarm that governments and private entities are expanding surveillance efforts and automating decision-making in ways that may be discriminatory.[34,35] Critics have argued that this approach avoids thornier questions about who should be allowed to use these algorithms, to what avail, and why they were built in the first place.[36,37]

To compel data processors to use data in a privacy preserving manner, the GDPR and the proposed PDP Bill place fiduciary obligations on the processors, expecting them to serve as trustees and act in the best interest of the data principals. NDHM allows data exchange between fiduciaries via a consent manager that allows the acquisition of asynchronous consent, or without, when mandated by law, as in case of emergencies. In theory, such pre-authentication

should allow data principals to “reflect on their choices” and make informed decisions about when and whom to share data with.[38]

The concept of the information fiduciary was proposed by Balkin and Zittrain in 2016 to place obligations on processors of data to adhere to purpose limitation (limit the scope of use), data minimisation (limit the collection and use to only what is necessary), storage limitation (limit the duration of use), and transparency.[39,40] By placing concrete obligations on data fiduciaries, the GDPR and the PDP Bill seek to mitigate the vulnerability created by power and information asymmetries between individuals and health professionals, large corporations, or the State.

Limitations

The fiduciary approach is not without its critiques. Drawing attention to the legally mandated obligation of corporations to their shareholders, Khan and Pozen[41] argue that data fiduciaries cannot always act in the best interests of data principals. Bailey and Goyal submit that a fiduciary duty to act in a person’s best interests does not necessarily prohibit the sale of their data for profit.[42] Except for data breaches, data fiduciaries are not mandated to report any legal transgressions under the PDP Bill.[43] A data principal can approach the “Data Protection Authority” if she believes that a data fiduciary has violated obligations. Thus, the onus of detection and enforcement remains with the data principal and may pose a challenge for individuals.

Time and purpose limitations could replicate the kind of undue unintended burden the Health Insurance Portability and Accountability Act, the law governing healthcare data in the United States, has placed on data flow for routine clinical care.[44] They are also in direct tension with the intent of machine learning algorithms to mine data to reveal novel biological or behavioural relationships.[45] The imposition on fiduciaries face some of the very challenges faced by consent-heavy frameworks: it is impossible to tell what the future holds for the data, and what future the data will reveal.

PRIVACY BY DESIGN

Recent advances in data science help address the limitations described above. Privacy by Design (PbD), a systems engineering approach first developed by Cavoukian in 1995, calls for proactive privacy preserving design choices embedded throughout the process lifecycle.[46] Since the advent of electronic medical records (EMRs), experts have recognised the need for embedding technological safeguards to protect privacy.[47] In many settings in India, personal data can often be easily accessed by people who do not need such access; for example clinic-based facilitators that may liaise with state or private insurance companies, insurance agents

themselves, and in the public sector, administrative officials. There is little recognition that such access, however unintentional or inadvertent, is unethical, and will very soon, be illegal.[48]

We have described below the dominant tools in current use that apply PbD principles to address gaps in health data protection [49]:

A. Data minimisation

When health data are collected, either through clinical operations or during research, there is temptation to collect more and not less, given the opportunitycosts associated with collecting these data, resulting in exhaustive datasets archived in the public and private health sector, that pose significant privacy risks.[48] Restricting data collection to the essentials has in fact been demonstrated to declutter and improve the user-interface, and consequently, user-experience and compliance, while reducing privacy risks[50]

B. Role-based access

Role-based access is a standard feature in most advanced EMRs.[51] Open source tools like Dataverse provide scientists differential access to research databases as well.[52] Multi-authority attribute-based encryption schemes (MAABE) allow role-based models to scale by allowing access to users based on a set of attributes, rather than on individual identities.[53,54] For example, by virtue of being a verified clinician (regardless of who), physicians are generally able to look up most medical records at their institution easily; by virtue of being a public health administrator (regardless of who), officers should have no access to personal health information; and by virtue of being a research lab, the team would have access to authorised de-identified data, provided third-party regulators can affirm the veracity of each of their attributes (clinician, administrator, researcher).[55] The Account Aggregator, a similar consent management framework already in play in India's fintech ecosystem, lends itself to such selective, verifiable, pre-authenticated access as has been proposed at the backbone for the NDHM.[56] Since user-consent can be sought asynchronously (prior to actual data processing), this model somewhat mitigates inadvertent coercion associated with point-of-care consent seeking. The NDHM seeks to verify attributes by developing and maintaining "registries" of providers.[57]

C. User preference

The GDPR facilitates data access by requiring companies to provide a Consent Management Platform to give users more control over their data, by selecting from a menu of data-use options. DEPA and the NDHM seek to empower users by allowing them to place revocable time and purpose limitations on the use of their data - the sorts of choices that would be extremely beneficial to patients. In theory, patients would control who accesses their data at all times, would receive notification of third-party access (whether authorised or not), or be able to revoke access at will, when permitted by law.

Others have elaborated on the idea by allowing data principals to opt into certain 'data trusts' or stewards with pre-negotiated access controls, where general attributes can be used to guide future data sharing: for example, a patient may elect to always allow healthcare providers to access her data but always deny access to pharmaceutical companies regardless of the identifiability of the data.[58,59,60]

D. Differential Privacy

There are a vast number of applications in both clinical care and scientific research that need high resolution aggregate data, where de-identification and anonymisation are not optimal solutions. Differential Privacy seeks to balance such access to rich data while preserving privacy. It achieves this balance by differentially introducing 'statistical noise' in the dataset, depending on what is being queried and by whom, thus combining the approaches described above. The 'noise' masks the contribution of each individual data point without significantly impacting the accuracy of the analysis. Moreover, the amount of information revealed from each query is calculated and deducted from an overall privacy budget to halt additional queries when personal privacy may be compromised. If effective, this approach will help alleviate some of the concerns about combining large datasets. There is already precedence for differential privacy as a model for collaborative research.[61] It can play a stabilizing role in the digital health system for clinical, operational and commercial applications. Open source platforms like OpenDP are likely to accelerate use of the application of differential privacy across disciplines.[62]

The PbD approaches described above seek to make the granting of consent more meaningful and manageable, while simultaneously making fiduciary uses of data more enforceable.

3. REGULATION

The jurisprudence on privacy is rapidly evolving in India (see Table 1), and includes a landmark judgement affirming the right to privacy.[63] The PDP Bill seeks to regulate the collection and transfer of all personal data, including health information. The law requires consent from the data principal before processing their personal data, and because health data are considered "sensitive" by the law, the data principal must be informed of any potential harm to them resulting from the processing of their data. It also requires fiduciaries to introduce technical safeguards through anonymisation and to adopt measures to prevent unauthorised access and misuse of the data, thus presenting a non-prescriptive opportunity to adopt privacy preserving design. Proposed policy and technology frameworks including the National Digital Health Blueprint[64] and Data Empowerment and Protection Architecture[65] (DEPA) seek to mitigate this consent-heavy environment, but are not legally enforceable.

Data that have been ‘irreversibly’ anonymised and do not fall within the scope of the PDP Bill are addressed by a proposed Non-Personal Data Governance Framework.[66] It recommends that fiduciary obligations remain in place even when personal data are anonymised, and that data principals should provide consent for both, anonymisation and the use of the anonymised data. The Framework seeks to create differentially accessed data commons distinguished by source of origin of the data: whether from individuals, communities, public domains, or private entities. While this may indeed be the holy grail of data access, the implementation path is uncertain in the absence of regulations.

Table 2 summarises the strengths and limitations of the four approaches described above, none of which can alone provide satisfactory data access while preserving privacy. Socioeconomic realities, technological ubiquity and the scope and nature of the regulatory environment will help communities calibrate the approaches that will best suit them. We favour the creation of an enabling regulatory environment where PbD principles can be leveraged not only to allow safe data exchange, but also to embed enforceability at scale.

DISCUSSION

The accelerated growth of data science in recent years has resulted in large shifts in societal responses to new technologies. The growing excitement over the interoperability of mobile apps was replaced with collective concern about data-grabs and unforeseen use of personal data that resulted in the GDPR. Some argue that it in turn places an undue burden on technology companies, inadvertently pushes out smaller players and gives larger data brokers a competitive advantage.[28] Just as several early adopters of virtual assistants have unplugged their devices and turned off their cameras, and many WhatsApp enthusiasts are migrating to Signal, it is not unreasonable to expect an ebb and flow in society’s embrace of health data exchange, as expectations and fears change with time. Low adoption of digital contact tracing apps during the coronavirus pandemic reflected the low levels of trust in technology platforms and in governments.[67] The technology and policy frameworks that eventually define health data ecosystems must therefore not only account for these tides but also acknowledge the local social contexts in which they are developed.[68] They must also account and accommodate for the inadvertent inequities that digitisation can exacerbate. Despite the perceived ubiquity of cell phones in India, only 502.2 million adults own smart phones, with the elderly, disabled and poor – those with likely the greatest health needs – having the least access.[69] Internet access in rural India is limited to one in three persons,[70] with significant gender disparity.[71]

CONCLUSION

Consent will remain the bedrock of information exchange in medicine for the foreseeable future. In its current avatar, however, consent is flawed and must be improved by applying intelligent

design to limit our ability to select harmful options. Legislation that mandates transparency and accountability will likely generate the trust needed to improve the adoption of digitisation. And trust will be the foundation of the kinds of data commons that must be built to advance the science of medicine and the health of populations.

References

1. Agarwal N, Jain P, Pathak R, et al. Telemedicine in India: A tool for transforming health care in the era of COVID-19 pandemic. *J Educ Health Promot* 2020;9:190. doi: 10.4103/jehp.jehp_472_20 [published Online First: 2020/09/22]
2. Mahajan V, Singh T, Azad C. Using Telemedicine During the COVID-19 Pandemic. *Indian Pediatr* 2020;57(7):652-57. [published Online First: 2020/05/16]

3. Ohannessian R, Duong TA, Odone A. Global Telemedicine Implementation and Integration Within Health Systems to Fight the COVID-19 Pandemic: A Call to Action. *JMIR Public Health Surveill* 2020;6(2):e18810. doi: 10.2196/18810 [published Online First: 2020/04/03]
4. Dagan A, Mechanic OJ. Use of ultra-low cost fitness trackers as clinical monitors in low resource emergency departments. *Clin Exp Emerg Med* 2020;7(3):144-49. doi: 10.15441/ceem.19.081 [published Online First: 2020/10/09]
5. Naslund JA, Shidhaye R, Patel V. Digital Technology for Building Capacity of Nonspecialist Health Workers for Task Sharing and Scaling Up Mental Health Care Globally. *Harv Rev Psychiatry* 2019;27(3):181-92. doi: 10.1097/hrp.0000000000000217 [published Online First: 2019/04/09]
6. Robertson FC, Lippa L, Broekman MLD. Editorial. Task shifting and task sharing for neurosurgeons amidst the COVID-19 pandemic. *J Neurosurg* 2020:1-3. doi: 10.3171/2020.4.jns201056 [published Online First: 2020/04/18]
7. National Digital Health Mission [Available from: https://ndhm.gov.in/ accessed January 17, 2021.
8. El Emam K, Rodgers S, Malin B. Anonymising and sharing individual patient data. *BMJ : British Medical Journal* 2015;350:h1139. doi: 10.1136/bmj.h1139
9. de Montjoye YA, Hidalgo CA, Verleysen M, et al. Unique in the Crowd: The privacy bounds of human mobility. *Sci Rep* 2013;3:1376. doi: 10.1038/srep01376 [published Online First: 2013/03/26]
10. Na L, Yang C, Lo CC, et al. Feasibility of Reidentifying Individuals in Large National Physical Activity Data Sets From Which Protected Health Information Has Been Removed With Use of Machine Learning. *JAMA Netw Open* 2018;1(8):e186040. doi: 10.1001/jamanetworkopen.2018.6040 [published Online First: 2019/01/16]
11. Brach C. Making Informed Consent an Informed Choice. Health Affairs Blog, April 4, 2019.
12. Shah A. Using data for improvement. *BMJ* 2019;364:l189. doi: 10.1136/bmj.l189
13. Ebeling MFE. Coercive Consent and Digital Health Information. Healthcare and Big Data: Digital Specters and Phantom Objects. New York: Palgrave Macmillan US 2016:67-94.
14. Faden RR, Beauchamp TL, King NMP. A History and Theory of Informed Consent: Oxford University Press 1986.
15. Manta CJ, Ortiz J, Moulton BW, et al. From the Patient Perspective, Consent Forms Fall Short of Providing Information to Guide Decision Making. *J Patient Saf* 2016 doi: 10.1097/pts.0000000000000310 [published Online First: 2016/08/05]
16. Pandiya A. Readability and comprehensibility of informed consent forms for clinical trials. *Perspect Clin Res* 2010;1(3):98-100. [published Online First: 2011/08/05]
17. Walker K. The costs of privacy. *Harv JL & Pub Pol'y* 2001;25:87.
18. Ploug T, Holm S. Informed consent and routinisation. *Journal of Medical Ethics* 2013;39(4):214-18.
19. Kaye J, Whitley EA, Lund D, et al. Dynamic consent: a patient interface for twenty-first century research networks. *Eur J Hum Genet* 2015;23(2):141-6. doi: 10.1038/ejhg.2014.71 [published Online First: 2014/05/08]
20. Jeffrey B, Walters CE, Ainslie KEC, et al. Anonymised and aggregated crowd level mobility data from mobile phones suggests that initial compliance with COVID-19 social distancing interventions was high and geographically consistent across the UK. *Wellcome*

Open Res 2020;5:170. doi: 10.12688/wellcomeopenres.15997.1 [published Online First: 2020/09/22]
21. Kishore N, Kiang MV, Engø-Monsen K, et al. Measuring mobility to monitor travel and physical distancing interventions: a common framework for mobile phone data analysis. *Lancet Digit Health* 2020;2(11):e622-e28. doi: 10.1016/s2589-7500(20)30193-x [published Online First: 2020/09/10]
22. Culnane C, Rubinstein BI, Teague V. Health data in an open world. *arXiv preprint arXiv:171205627* 2017
23. Sloan RH, Warner R. Beyond notice and choice: Privacy, norms, and consent. *J High Tech L* 2014;14:370.
24. Solove DJ. The digital person: Technology and privacy in the information age: NYU Press 2004.
25. Nissenbaum H. A contextual approach to privacy online. *Digit Enlight Yearb* 2012:219-34.
26. General Data Protection Regulations. 2016/679.
27. The Personal Data Protection Bill. 373 of 2019: Lok Sabha, 2019.
28. Chivot E, Castro D. The EU Needs to Reform the GDPR To Remain Competitive in the Algorithmic Economy: Center for Data Innovation, May 13 2019.
29. Partnership on AI [Available from: https://www.partnershiponai.org/about/ accessed January 17, 2021.
30. NSF. NSF Program on Fairness in Artificial Intelligence in Collaboration with Amazon (FAI): National Science Foundation, 2020.
31. Microsoft. Microsoft AI Principles [Available from: https://tinyurl.com/y3g4zz54 accessed January 17, 2021.
32. Google. AI at Google: Our Principles 2018 [Available from: https://www.blog.google/technology/ai/ai-principles/ accessed January 17, 2021.
33. Olson P. Google Quietly Disbanded Another AI Review Board Following Disagreements: The Wall Street Journal; April 16, 2019 [Available from: https://www.wsj.com/articles/google-quietly-disbanded-another-ai-review-board-following-disagreements-11555250401?st=8djs0dshthp1z05 accessed January 17, 2021.
34. Murray SG, Wachter RM, Cucina RJ. discrimination by artificial intelligence in a commercial electronic health record—a case study. *Health Affairs Blog* 2020;10
35. Obermeyer Z, Powers B, Vogeli C, et al. Dissecting racial bias in an algorithm used to manage the health of populations. *Science* 2019;366(6464):447-53. doi: 10.1126/science.aax2342
36. Whittaker M, Crawford K, Dobbe R, et al. AI Now Report 2018. New York, NY: AI Now Institute, 2018.
37. McLennan S, Lee MM, Fiske A, et al. AI Ethics Is Not a Panacea. *The American Journal of Bioethics* 2020;20(11):20-22. doi: 10.1080/15265161.2020.1819470
38. Coiera E, Clarke R. e-Consent: The design and implementation of consumer consent mechanisms in an electronic environment. *J Am Med Inform Assoc* 2004;11(2):129-40. doi: 10.1197/jamia.M1480 [published Online First: 2003/12/10]
39. Balkin J, Zittrain J. A Grand Bargain to Make Tech Companies Trustworthy. The Atlantic, October 3, 2016.
40. Balkin JM. The Fiduciary Model of Privacy. *Harvard Law Review Forum* 2020;134(1)
41. Khan LM, Pozen DE. A skeptical view of information fiduciaries. *Harv L Rev* 2019;133:497.

42. Bailey R, Goyal T. Fiduciary relationships as a means to protect privacy: Examining the use of the fiduciary concept in the draft Personal Data Protection Bill, 2018., 2019.
43. Reddy P. Personal Data Protection Bill: Notification Of Data Breaches: Bloomberg Quint; 2020 [Available from: https://www.bloombergquint.com/opinion/how-the-personal-data-protection-bill-tackles-data-breaches accessed January 17, 2021.
44. Nosowsky R, Giordano TJ. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule: Implications for Clinical Research. *Annual Review of Medicine* 2006;57(1):575-90. doi: 10.1146/annurev.med.57.121304.131257
45. Mittelstadt BD, Floridi L. The ethics of big data: current and foreseeable issues in biomedical contexts. *Science and engineering ethics* 2016;22(2):303-41.
46. Cavoukian A. Privacy by design: The 7 foundational principles: The International Association of Privacy Professionals, 2009.
47. Rindfleisch TC. Privacy, information technology, and health care. *Commun ACM* 1997;40(8):92–100. doi: 10.1145/257874.257896
48. Sahay S, Mukherjee A. Where Is All Our Health Data Going? *Economic & Political Weekly* 2020;55(1):47.
49. van Rest J, Boonstra D, Everts M, et al. Designing Privacy-by-Design. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014:55-72.
50. Balsari S. Will AI help universalize health care? : BMJ Opinion; September 23, 2019 [Available from: https://blogs.bmj.com/bmj/2019/09/23/satchit-balsari-will-ai-help-universalize-health-care/ accessed January 17, 2021.
51. de Carvalho Junior MA, Bandiera-Paiva P. Health Information System Role-Based Access Control Current Security Trends and Challenges. *Journal of Healthcare Engineering* 2018;2018:6510249. doi: 10.1155/2018/6510249
52. King G. An Introduction to the Dataverse Network as an Infrastructure for Data Sharing. *Sociological Methods and Research* 2007;36:173–99.
53. Wickramasuriya J, Venkatasubramanian N. Dynamic Access Control for Ubiquitous Environments. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004:1626-43.
54. Yu S, Ren K, Lou W, et al. Security and Privacy in Communication Networks: Berlin, Germany: Springer, 2009.
55. Jiang S, Zhu X, Wang L. EPPS: Efficient and Privacy-Preserving Personal Health Information Sharing in Mobile Healthcare Social Networks. *Sensors (Basel)* 2015;15(9):22419-38. doi: 10.3390/s150922419 [published Online First: 2015/09/26]
56. Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016 [Available from: https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=3142 accessed January 17, 2021.
57. NDHM Health Facility Registries FAQ [Available from: https://ndhm.gov.in/home/health_facility_registry_faq accessed January 17, 2021.
58. Delacroix S, Lawrence ND. Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance. *International Data Privacy Law* 2019;9(4):236-52. doi: 10.1093/idpl/ipz014
59. Tentori M, Favela J, Rodriguez MD. Privacy-aware autonomous agents for pervasive healthcare. *IEEE Intelligent Systems* 2006;21(6):55-62.
60. Rosenbaum S. Data Governance and Stewardship: Designing Data Stewardship Entities and Advancing Data Access. *Health Services Research* 2010;45(5p2):1442-55. doi: 10.1111/j.1475-6773.2010.01140.x

61. Dwork C. Differential privacy: A survey of results. International conference on theory and applications of models of computation: Springer, 2008:1-19.
62. OpenDP. OpenDP: Building an open-source suite of tools for deploying differential privacy 2020 [Available from: https://projects.iq.harvard.edu/opendp accessed January 17, 2021.
63. Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India. Supreme Court Cases: Supreme Court of India, 2017:1.
64. National Digital Health Blueprint: Ministry of Health and Family Welfare; [Available from: https://main.mohfw.gov.in/sites/default/files/Final%20Report%20-%20Lite%20Version.pdf accessed January 17, 2021.
65. Niti-Aayog. Data Empowerment and Protection Architecture: Draft for Discussion 2020 [Available from: https://niti.gov.in/sites/default/files/2020-09/DEPA-Book_0.pdf accessed January 17, 2021.
66. MEITY. Report by the Committee of Experts on Non-Personal Data Governance Framework: Ministry of Electronics and Information Technology, Government of India, 2020.
67. Combating COVID-19: Lessons from Singapore, South Korea and Taiwan: Knowledge@Wharton; 2020 [Available from: https://knowledge.wharton.upenn.edu/article/singapore-south_korea-taiwan-used-technology-combat-covid-19/ accessed January 17, 2021.
68. May C, Mort M, Williams T, et al. Health technology assessment in its local contexts: studies of telehealthcare. *Social science & medicine* 2003;57(4):697-710.
69. Silver L, Smith A, Johnson C, et al. Mobile Connectivity in Emerging Economies: Pew Research Center, March 2019.
70. Kawoosa VM. Connectivity gets better but parts of India still logged out. *Hindustan Times* August 14, 2020.
71. Bhuyan A. 4 In 5 Bihar Women Have Never Used The Internet December 16, 2020 [Available from: https://www.indiaspend.com/gendercheck/4-in-5-bihar-women-have-never-used-the-internet-702855 accessed January 17, 2021.

Table 1

Document	Details	Type	Nature
Puttaswamy v. Union of India	Judgment of the Supreme Court of India affirming the right to privacy of all individuals under the Indian Constitution.	Law	Binding
Information Technology Act, 2000	Prescribes security practices for the protection of personal data. Requires that consent must be sought before the collection of any sensitive personal data.	Law	Binding and Enforceable
HIV/AIDS Act 2017, Mental Healthcare Act, 2017, Transplantation of Human Organs and Tissues Act, 1994	Sector-specific laws that govern data related to the disease area. The requirements may be different from those under the IT Act	Law	Binding and Enforceable
Personal Data Protection Bill, 2019	Proposed law that updates the IT Act and protects all personal data, establishes a data protection regulator and prescribes penalties for violations of these rules.	Bill; Pending in Parliament	Unenforceable till passed as law
Data Empowerment and Protection Architecture	Framework for data management and security issued by NITI Aayog, a government think-tank	Draft Report	Voluntary

National Digital Health Blueprint	Lays out the architectural framework for the digital health infrastructure under the National Digital Health Mission	Government Report	Voluntary
Report by the Committee of Experts on Non-Personal Data Governance Framework	This Committee of Experts was constituted by the Ministry of Electronics and Information Technology to propose a governance framework for non-personal data. It has released a draft report for public comments (July 2020).	Draft Government Report	Recommendations to the Government

Table 2

Approach	Strength	Limitation
Consent-framework	1 Traditionally and widely used as a tool to ensure patient autonomy and (despite its limitations) prevent exploitative practices 2 In common use by medical practitioners during the provision of routine healthcare, or researchers during research projects 3 The ethical and legal framework for consent is well established. 4 No additional costs need to be	1 It currently takes the form of lengthy and complicated consent forms that the patient may not properly read or understand. With consent needed for many actions during a medical procedure, consent may sometimes be given without due consideration or out of habit. 2 In the context of healthcare, a power differential exists between the patient and medical provider. It is therefore unclear how truly autonomous consent is. 3 It is impossible for the patient to consent to all the possible uses of

	incurred as it is already a part of patient care.	the data, which might not be known at the time that it is being collected. Re-consent may not be possible if data has been anonymised or the patients might not be contactable. This may hinder medical research and the development of novel technologies.
Fiduciary Obligations	1 Instead of the onus for data protection being on patients, shifts this burden onto entities collecting, storing and using the data 2 Particularly useful where the ability of the patient to provide informed consent is impaired such as in the context of deidentified or anonymised data where there is a potential for a privacy violation if the data is made identifiable or is de-anonymised.	1 It may be difficult for a data principal to detect that an entity processing their data has violated a fiduciary duty. 2 These obligations may conflict with legally enforceable the duties that corporations owe to their shareholders 3 Might be difficult to enforce since large quantities of data would have to be regulated. In India, it will require a strong and independent data protection authority.
Privacy by Design	1 Reduces the chance of human-induced errors by baking privacy preserving practices and features into the technical architecture	1 There is currently a lack of expert consensus or comprehensive guidelines from data protection authorities on the kinds of safeguards that must be incorporated in enterprise architecture for healthcare. 2 Might increase operational costs for healthcare organisations. This would disproportionately affect smaller organisations. 3 Has not yet been formally incorporated into the information systems of major health IT companies or health systems of countries.

Regulation	1 Provides clear guidelines to protect the privacy rights of people and an environment of legal and operational certainty for entities processing data 2 Rights can be enforced using legal mechanisms and penalties may be imposed for egregious violations of data protection obligations	1 Regulations may differ in different countries, increasing costs of compliance for entities operating internationally 2 If the regulations are too burdensome, it may limit innovation 3 Large costs imposed by data protection regulators may affect smaller organisations but would be insignificant for big companies like Facebook and Google. 4 Since privacy is legally understood as an individual right, it may be difficult to protect group privacy under this framework