The Dialogue™
INFORM ENGAGE IDEATE

May, 2022

HEALTH DATA MANAGEMENT POLICY

RESPONSE

Authored by Eshani Vaidya, Kamesh Shekar

Edited by Sreyan Chatterjee

TABLE OF CONTENTS

I. Thematic Responses to the Health Data Management Policy 2.0

A. Absence of a Legislative Mandate

In the absence of an comprehensive regulatory framework, implementation process and infrastructure act as regulation, substituting for or displacing parliamentary law.[1] Implementation processes, , can create path dependencies, foster cooperation, or structure conflict resolution.[2] In the case of India's public-interest technology, such as the ABDM, the plumbing of the digital health ecosystem is functioning as regulation, instead of the system being developed on the foundation of an ex-ante regulatory framework. A legislation with built-in accountability and transparency measures is an important step towards building a citizen-centric framework that can produce the desired outcomes. However, a framework that is restricted to responsiveness, evaluation and accountability may not have the same flexibility as one that has a legal mandate to establish rights, deliniate responsibilities and to provide remedies. Remedies and iterative stakeholder participation are essential elements of effective accountability practices.[3]

An accountability framework backed by codified law must, therefore, take into consideration the exisiting workflows of those within the system. The absence of clearly defined roles and responsibilities may pave the way for discretionary use of authority. When dealing with sensitive personal data, like health data, providing for the categories of collection and data flows is not enough to create a strong data protection framework.

B. Governance Framework

The NHA (as a nodal body) and the ABDM (as an eco-system) are both backed by Cabinet decisions, i.e., an executive mandate. The intention to draft a legislation to support these systems was expressed in 2019[4] but has not come to fruition. As a non-statutory body

[1] Benedict Kingsbury, Infrastructure and InfraReg: on rousing the international law 'Wizards of Is', 8 Cambridge International Law Journal 171-186 (2019).

[2] Benedict Kingsbury, Infrastructure and InfraReg: on rousing the international law 'Wizards of Is', 8 Cambridge International Law Journal 171-186 (2019).

[3] Walter Flores, Community Monitoring for Accountability in Health: Review of Literature, Open Society Foundations (2011), https://www.copasah.net/uploads/1/2/6/4/12642634/literature_review_community_monitoring_social_accountability_in_health.pdf

[4] From National Health 'Agency' to 'Authority': Ayushman Bharat Body Restructured Yet Again, The Wire (Jan. 3, 2019), https://thewire.in/government/ayushman-

performing a crucial public function, it is important to clarify the scope of NHA's mandate and the checks on powers that they are required to wield.

The National Health Authority has been entrusted with, among other things, designing strategy, building technological infrastructure, and implementing the 'Ayushman Bharat Digital Mission' to create a National Digital Health Ecosystem. The previous iteration of the Health Data Management Policy ('**HDMP**') had granted the NHA the authority to formulate subordinate rules and guidelines within the ABDM. However, in its recent iteration, the HDMP has replaced most mentions of the 'NDHM' (in its earlier avatar) with that of the 'NHA'. For instance, the NHA is now granted the authority to 'specify the procedure for permitting different classes of entities such as data fiduciaries, data processors, Health Information Providers, Health Information Users and respositories to operate in the National Digital Health Ecosystem (NDHE)'.[5] The NHA must also specify the purposes for collection or processing of personal data.[6] It is unclear to what extent the NHA is being envisaged as a regulator of the eco-system (similar to say how UIDAI regulates Aadhaar eco-system) or as a nodal participant (similar to how NPCI supports the UPI eco-system). In our view, considering the importance of the HDMP, a formalised regulatory role should be carved out for the NHA.

C. Inclusivity

A citizen-centric approach to building a digital health data management eco-system must provide for citizens to have agency to claim and exercise their rights, to be informed regarding their choices, demand services, and seek redressal of their grievances. However, in the absence of awareness building, education, and adequate policies which are clearly communicated, an information asymmetry is created that makes the eco-system less responsive instead of more accessible. An opaque system can lead to a widening gap between the citizen and the regulator , damaging the feedback loops between them.[7]

---

bharat-national-health-agency-to-authority.

[5] ABDM, Draft Health Data Management Policy Version 2 (2022), Cl. 5.1.

[6] ABDM, Draft Health Data Management Policy Version 2 (2022), Cl. 9.3.

[7] Bidisha Chaudhuri, Distant, opaque and seamful: seeing the state through the workings of Aadhaar in India, 27 Information Technology for Development 37-49 (2020).

Keeping in mind the resource-limited conditions of most of the areas in India, in addition to the challenges of digital penetration, it is important to create an ecosystem that puts end-user accessiblilty first. For example, the digital ID issued must not require any links to Aadhaar for authentication and subsequently, to obtain welfare benefits. In order to ensure continuity of care, the system must empower healthcare providers to issue temporary IDs that can be subsequently linked to a consent manager.

II. Data Protection Regulation and the Health Data Management Policy

As health information is one of the sub-set of sensitive personal data[8] under upcoming data protection regulations, all the players within the ABDM, including the National Health Authority (unless exempted under Clause 35), will come under the ambit of the Data Protection Authority (DPA). This overlap of responsibility needs to be clarified.

The HDMP provides data principals with the right to portability, access and confirmation, and disclosure. In addition to the rights discussed in HDMP, the upcoming data protection regime provides a set of digital rights to the data principals, including the right to correction and erasure, and the right to be forgotten. It is unclear whether crucial rights vested through the upcoming data protection regime will be enforced under HDMP. Therefore to remove confusion, HDMP must align its provisions related to digital rights (and its exercising process) with that of upcoming data protection regulation. This has been iterated in the HDMP as well, where entities brought within the ambit of the HDMP must 'adhere to and comply with' laws, rules and regulations and standards pertaining to data protection that are in force in India.

HDMP and the upcoming data governance framework and PDP Bill outline different grievance management systems for data fiduciaries (refer to the below table), creating overlaps and confusion for stakeholders. An harmonisation process of the grievance mandates regarding the point of contact. The timeline for resolution under the two frameworks are harmonised (see table below). Additionally, as the Data Protection Bill, 2021 ('**DPB 2021**') states that the data principal can reach DPA[9] with complaints under Clause 69, functions of ABDM-Greviance Redressal Officer must be harmonised with the functions of the DPA.

[8] Ministry of Electronics and Information Technology, Draft Personal Data Protection Bill, 2019, Cl. 3(36)

[9] Joint Parliamentary Committee, Draft Data Protection Bill, 2021, Cl. 32(4)

Table 1: Grievance redressal mechanisms

Legislation	Provisions	Mandate	Point of Contact for Consumers	Time Duration for Resolution
Personal Data Protection Bill, 2019 (PDP Bill)	Clause 32	Data fiduciary to have effective grievance mechanisms to redress data principals complaints efficiently in a speedy manner	Data protection officer (in the case of significant data fiduciary) Any designated officer (in case of data fiduciary)	No later than thirty days from the date of receipt
Health Data Management Policy	Clause 32	Data fiduciary to have effective grievance mechanisms to redress data principals complaints efficiently in a speedy manner	Data Protection Officer	Within one month from the date of receipt of the grievance.
Draft Non-Personal Data Governance Framework	Point 7.7(ii)	Data trustee is obligated to establish grievance redressal mechanisms for the community.	-	-

The expert committee on non-personal data proposed to set up a national-level regulation that will (i) vest rights over non-personal data, (ii) enable data sharing to unlock the economic benefits from NPD, and (iii) address privacy, re-identification of anonymised personal data,

and prevent misuse of and harms from data.[10] As HDMP lays out the mechanism for sharing de-identified or anonymised data by data fiduciaries[11], it is crucial to align this process with the NPD governance framework.

As Health Information Exchange & Consent Manager ('**HIE-CM**') would act as a consent manager for health information transfer, they would fall within the ambit of DPA[12] as they have to register under the authority. This highlights the overlapping scope, which would result in regulatory arbitrage and confusion. This overlap needs to be resolved to ensure a seamless health information transfer pipeline.

Recommendations for PDP Harmonisation:

1. Regulating and securing health data falls within the ambit of DPA, therefore HDMP and subordinate guidelines and rules must be finalised with consultation with the DPA.
2. HDMP must harmonise the grievance mandates regarding point of contact with the upcoming data protection regulation and governance framework.
3. Mechanism proposed for sharing de-identified or anonymised data by data fiduciaries, must be aligned with the NPD governance framework.
4. NHA must work in tandem with DPA to sketch out provisions and guidelines for HIE-CM to have a seamless health information transfer pipeline.

[10] Ministry of Electronics and Information Technology, Report by the Committee of Experts on Non-Personal Data Governance Framework, Cl. 3.6.

[11] ABDM, Draft Health Data Management Policy Version 2 (2022), Cl. 29.

[12] Ministry of Electronics and Information Technology, Draft Personal Data Protection Bill, 2019, Cl. 23(5).

IV. Clause Specific Analysis of the Health Data Management Policy

Relevant Provision of HDMP	Digital Healthcare Principle	Healthcare Intervention	Rationale	Additional References
Data Protection Measures				
Definitions Clause 4	Develop a Clear Taxonomy *Developing a clear taxonomy for within the ecosystem will allow for the development of standards and improve compliance at large.*	- Provide express definitions for the following terms: a) Health Locker b) Consent Manager c) Pseudonymisation (*These were defined in the previous version of the HDMP)*	1. Health Locker has been provided for in the NDHM Strategy Overview[13] and the NDHM Guidelines for Health Information Providers, Health Repository Provider and Health Locker. Health lockers can store personal health records (as it provides an optional service)[14] and the manner of storage, data protection and access must be	The Dialogue's response to the first draft HDMP also recommends: 1. Provide a definition for health data; 2. Ensure key terms are not left undefined (such as point of care, health locker; and 3. Ensure harmonisation of definitions against different data protection regulations in the country.[15]

[13] ABDM, Draft Health Data Management Policy Version 2 (2022), Cl. 2.2.8.

[14]National Health Authority, Implementing Health Lockers: NDHM Webinar 5, ABDM Sandbox, https://sandbox.abdm.gov.in/webinars/Health_locker_webinar.pdf

[15] The Dialogue, Response to the Draft Health Data Management Policy (2021).

			expressly provided for. 2. Consent Managers have been remodelled as "Health Information Exchange-Consent Manager". The existing framework allows the consent manager to process data fiduciary requests and consent mechanisms. It is important to clearly define whether or not an HIE-CM will function as an intermediary or an active participant so as to assign appropriate liability.	
Rights of a	Rights of a Data	- Expressly provide for the right to opt-in and opt-	The rights granted to	In the absence of an express

Data Principal Clause 14	Principal *The right to opt-in and opt-out of the ecosystem must be expressly provided to the data principal.*	out of the UHID or any other registries within the ABDM. - This must be accompanied with the following rights: a) Right to correction/erasure[16] information related to the data principal, which is guaranteed under PDP Bill.[17] b) Right to revoke consent; and c) Right to be forgotten which is guaranted under PDP Bill[18] and vested through Puttaswamy II judgement.[19] .	the data principal must be expressly mentioned in the HDMP and in privacy notices[20] in order to ensure there is a reduction of information asymmetry, and to increase accountability.	mandate, it is likely that data principals are unaware of their rights and therefore cannot enforce accountability. In the United States, the Privacy Rule applies. This grants data principals rights over their health information. These have been clearly laid out in HIPAA, in addition to the IEC-based efforts undertaken via the website.[21]

[16] Though HDM Policy nebulously mentions under the Data Quality principle that "Personal data once created cannot be erased or amended without following the due process referred to in Clause 14.2 of this Policy", it does not explicitly list the right to correction and erasure within the Clause 14.

[17] Ministry of Electronics and Information Technology, Draft Personal Data Protection Bill, 2019, Cl. 18.

[18] Ministry of Electronics and Information Technology, Draft Personal Data Protection Bill, 2019, Cl. 20.

[19] In 2018, the Supreme Court recognised the "right to be let alone" as a postulate of the "right to privacy" through Justice K.S.Puttaswamy(Retd) vs Union Of India (Puttaswamy Judgement II) verdict with reasonable exemptions.

[20] Shefali Malhotra et. al., Analysing the Health Data Management Policy: Working Paper (2021) Internet Freedom Foundation & Centre for Health Equity Law and Policy.

[21]Your rights under HIPAA, Health and Informational Privacy, U.S. Department of Health & Human Services, https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html.

Consent Framework Chapter III	Informed Consent *The ABDM must provide for consensus ad idem, which means the relevant parties 'must agree to the same thing in the same sense'.*[22]	- Require consent even in instances of digitisation of records, not simply in the context of changes in the purpose of collection. - Expressly include 'revocation of consent' as one of the rights a data principal holds (under cl. 14 of the HDMP). - The privacy notice should contain the following: a) Implications of granting/refusing consent; b) Explainers that detail the flow of data throughout its life cycle; and c) An option to contact a person/centre that can assist with a more detailed understanding of the same. - The burden of proof of consent must lie with the data fiduciary. - Ensure time-period and outcome-based consent mechanisms that allow for access only for a specified duration.[23]	A 'notice and consent' mechanism has become the heart of privacy law today. These are a few measures that will allow individuals to appropriately operationalise consent. Additionally, the Personal Data Protection Bill, 2019 states that the burden of proof of consent must lie with the data fiduciary.[24]	The consent framework as seen in the US HIPAA distinguishes between 'consent' and 'authorization'. Consent means patient consent for uses and disclosures of health information for treatment, payment, and healthcare operations. An authorization, on the other hand, is for a use or disclosure not otherwise permitted by the Legislation.[25]
Sharing of De-	Anonymisation	- A Standard Operating Procedure (SoP) should be	While anonymisation	The United States differentiates

[22]As provided for under the Indian Contracts Act, 1872.

[23]Sreyan Chatterjee et. al., India's Digital Health Dreams: Getting it Right (Apr. 2022) The Dialogue, https://thedialogue.co/wp-content/uploads/2022/04/Indias-Digital-Health-Dreams.pdf.

[24]Ministry of Electronics and Information Technology, Draft Personal Data Protection Bill, 2019.

[25]U.S. Department of Health and Human Services, What is the difference between "consent" and "authorization" under the HIPAA Privacy Rule? (HHS.Gov, Aug. 2021), https://www.hhs.gov/hipaa/for-professionals/faq/264/what-is-the-difference-between-consent-and-authorization/index.html.

identified or Anonymised Data by Data Fiduciaries Clause 29	*Development of standards of anonymisation is an essential practice within such critical infrastructure.*	developed. - The SoP must define bright lines for sharing anonymised data, decide on an appropriate anonizmysation standard which takes privacy risks into consideration. - Uniform standards of anonymisation must be adopted as a first step towards data protection. These must delineate the distinction between 'anonymised data' and 'deidentified data' (definition and relevant processes).	of data is the first step towards data protection, enforcement of standards will allow for a uniform approach, which also makes enforcement more efficient.	between authorization and access. HIPAA provides that the data controller must certify that they had no 'actual' knowledge that the residual information can be used to identify an individual. Of course, the determination of 'actual knowledge' comes with another set of challenges. HIPAA fails to specify the acceptable level of risk of identification is, therefore cannot clearly define 'appropriate knowledge and experience'.
Data fiduciaries must provide for purpose of collection of data Clause 26.3	Purposes of Collection *As established in Justice K.S. Puttaswamy v. Union of India (2017)*	- Privacy impact assessments, conducted independently, must form part of the consent framework. - These must take place at a federated level, depending on the nature of data collected. - A legal mandate must expressly provide for the scope of collection of health data and the strict limitations applied. At present, the onus of marking out these limitations lies with data	This will work towards ensuring that the principles of limitation, minimisation and others established by Indian privacy jurisprudence[27] are followed.	The National Health Service in the United Kingdom had developed a collaborative programme with DeepMind, a private entity without appropriate data protection safeguards. This collaboration was criticised by several observers on the ground that

[27]Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

		fiduciaries.[26] - These limitations must also apply in case of private parties acting as data fiduciaries.		the 'appropriate use' of a public resource was not expressly laid down in law or policy.[28]
Processing Personal Data Pertaining to a Child Clause 12	Minors Right to Erasure and Consent *The policy must clearly lay down the the working of the health registries when minors attain the age of majority.*	- Provide minors with a contingency plan in case the minor: a) Does not wish to partake in the digital health ecosystem once they attain the age of majority; b) Does not have a legal representative (parent/gaurdian) within the health ecosystem.[29]	Minors should be excluded from availing of health related services or patient care in the absence of a parent or guardian.	The JPC Report on the Draft Personal Data Protection Bill, 2019 provides for the manner in which data fiduciaries must treat consent granted by minors. For instance, three months before attaining the age of majority, the data fiduciary must inform the child about providing consent again.[30]
ABHA (number) Chapter IV	Allocation of ABHA Number to Minors *It is important to detail the process in*	- An express provision must detail the manner in which minors can be allocated an ABHA number. - The process must detail the following: a) Consent Mechanism (with or without a parent/guardian);	In addition to collecting personal data of minors, it is important to clearly outline their participation in the	In the absence of ABHA, it is important to ensure that the minor can become a wilful participant in the ABDM. If at all minors do not need a health ID, detailing exceptions will

[26]ABDM, Draft Health Data Management Policy Version 2 (2022), Cl. 26.2.

[28] Angela Ballantyne & Cameron Stewart, Big Data and Public-Private Partnerships in Healthcare and Research: The Application of an Ethics Framework for Big Data in Health and Research, 11 Asian Bioethics Rev. 315, 326 (2019).

[29]IT for Change, Response to the Public Consultation on the draft Health Data Management Policy (Sept. 2020).

[30]Cl. 1.15.11.3, Lok Sabha Secretariat, Report of the Joint Committee on the Personal Data Protection Bill, 2019 (Dec. 2021), Seventeenth Lok Sabha, http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf.

	which minors can be granted an ABHA number.	b) Access to healthcare and welfare schemes in the absence of an ID; and c) Continuity of care upon attaining the age of majority.	ABDM. This will allow for appropriate delineation of rights and duties.	ensure there is little ambiguity in the manner in which data fiduciaries and other stakeholders must treat minors health information.
Risk Management				
Privacy Principles to be followed by Data Fiduciaries Clause 26	Graded Health Data Sets *Graded health data classification will allow for particular assignment of rights and liabilities.*	- Classification of data sets must be done in the following manner: a) Based on the nature of data–personal, anonymised and non-personal data. b) Additionally, anonymised and de-identified data must be classified as distinct from one another. c) Assessing risk based on associated transactions (such as operational information, health records etc.) - The process of determining such classification must constitute a feedback mechanism that is consultative in nature.	Patient data comprises data that can be shared and data that is highly sensitive in nature, often associated with a considerable social stigma. Additionally, anonymised data is entirely de-linked from personally identifiable information, while de-identified data still maintains links to sensitive information. Therefore, they must be treated with varying degrees of liability.	The Data Retention Guidelines[31] have noted the importance of a 'graded' approach towards the classification of health data sets.
Privacy Principles to	Bridging the Knowledge Gap in	- Classify stakeholders and data fiduciaries in terms of risk assessment (*See: Graded health data sets)*	Increased awareness within the	The Personal Data and Information Privacy Code,

[31]National Health Authority, Consultation Paper on Proposed Health Data Retention Policy (2021), https://abdm.gov.in:8081/uploads/Consultation_Paper_on_Health_Data_Retention_Policy_21_28557f9a6a.pdf.

be followed by Data Fiduciaries Clause 26	Cybersecurity *Improve reporting mechanisms and training programmes so as to teach stakeholders how they can effectively operationalise privacy and security standards.*	frameworks. Enforce and develop uniform reporting standards across each sub-sets thus created. - Collate and make publicly available continuous data on cyberattacks so as to identify vulnerabilities. - Conduct resilience and confidence building initiatives in addition to encouraging private actors on training their employees through information and tool sharing.	cybersecurity space allows actors to understand the threat landscape and develop innovative ways of improving privacy and security frameworks.	2019 that was tabled in the Lok Sabha, includes the right to access information about security breaches.[32]
Privacy Principles to be followed by Data Fiduciaries Clause 26	Cybersecurity *Building ex-ante measures and adopting a holistic approach towards cybersecurity management.*	- Healthcare supply chains should be developed as critical infrastructure in order to develop privacy and security standards that reflect that. - Ex ante measures must be undertaken to strengthen the existing cybersecurity mechanism (lack of trained personnel, outdated infrastructure) - Invest in user protection services (such as supporting victims of cyberattacks and developing adequate grievance redressal mechanisms)	Adoption of cybersecurity measures after the fact are important, but without preventative measures in place they will not have the desired impact. Health data is particularly susceptible to cyber attacks.	A study pointed out that hospitals that had faced data breaches in the last 3 years suffered a higher mortality rate. Cyberattacks have a significant impact on the day-to-day physical operations of a hospital.[33]
Audit Clause 27.5	Local Audit Frameworks *Enforcing audit trail management will*	- Create mandatory audit trail policies that are binding on all tertiary healthcare providers. The policy must work to ensure that datasets: a) Have accurately completed and properly	Allows for more effective, iterative policymaking and management	Audit trails help in maintaining complete and comprehensive information about patient data access. In Portugal, "in-demand

[32] Shefali Malhotra et. al., Analysing the Health Data Management Policy: Working Paper (2021) Internet Freedom Foundation & Centre for Health Equity Law and Policy.

[33]The CyberPeace Institute, Playing with Lives: Cyberattacks on Healthcare are Attacks on People , (Mar. 9 2021).

	enhance accountability.	structured essential fields; b) Are subjected to consistent data review; c) Maintain traceable access controls and automated immutable, credible and secure logbooks; and d) Maintain secure backups with similar access controls. - Promote the role of Hospital Chief Information Officers at the tertiary level who are responsible for AT management.	surrounding EHRs. Limits the power differential between healthcare providers and patients to ensure accountability. Allows for local adjustments and ensures that digitisation takes place in practice.	access to clinical information is still inadequate in many settings, contributing to duplication of effort, excess costs, adverse events, and reduced efficiency."[34] "While Portuguese emergency departments believed patients would benefit from the use of longitudinal records, they only accessed that information in 10% of cases."[35]
Entities under the NDHE and Applicable Laws Clause 5.3.	Establishing stadards for cybersecurity *Adherence to uniform standards allows for a more cohesive cybersecurity regime in the country.*	- Data fiduciaries must implement the International Standard IS/ISO/IEC 27001 on 'Information Technology – Security Techniques – Information Security Management System – Requirements.	Following a uniform set of standards (domestic and international) will allow for smoother cross-border data transfers.	Version 1 of the Draft HDMP mandates adherence to the International Standard (*see intervention).*[36]
Community				

[34]Cruz-Correia et al., Analysis of the quality of hospital information systems audit trails, BMC Medical Informatics and Decision Making (2013).

[35]Cruz-Correia et al., Analysis of the quality of hospital information systems audit trails, BMC Medical Informatics and Decision Making (2013).

[36]ABDM, Draft Health Data Management Policy Version 2 (2022), Cl. 27(1)(d).

Grievance Redressal and Compliance Chapter VII	Grievance Redressal *Citizens have the right to a timely, responsive and effective grievance redressal mechanism.*	- An overarching grievance redressal mechanism must be set up by the State and should be guaranteed by legislation. - The mechanism must provide for a step-wise approach towards escalation of complaints, with the first point of contact being decided in congruence with PDP Bill and NDP Governance framework. - Establish clear processes: a) Provide for a time limit within which the issue must be addressed; b) Issue a complaint number that allows citizens to track progress; and c) In order to be more inclusive, complaints should also be accepted via hotlines.	The grievance redressal mechanism must be provided for by the State so as to ensure fair treatment. A data fiduciary setting up it's own grievance redressal mechanism is problematic because: a) That will not allow data principals uniform redress; and b) There is no way to ensure the data fiduciary remains independent within this mechanism.	The UK's grievance redressal mechanism expressly (with statutory mandate, and different procedural requirements)[37] categorises its complaints as (i) against NHS Digital staff or (ii) against any aspect of NHS care treatment and service. For secondary care, local commissioning groups are contacted. For complaints about public health institutions, local authorities are contacted. If the problem persists, one can complain to the relevant ombudsman, including the Parliamentary and Health Service Ombudsman.[38]
ABHA and Other ID Policy	Temporary Health ID *This allows continuity*	- Ensure that paper-based consent mechanisms are in place, including access to a consent manager for those issued a temporary ID.	As seen in the Kerala e-health system, patients often do not have access to their	Clause 8(a) of the 2022 Policy states that '*Data principals should at all times have control and decision-making power over the manner in*

[37] The Local Authority Social Services and National Health Service Complaints (England) Regulations 2009, https://www.legislation.gov.uk/uksi/2009/309/contents/made.

[38] National Health Service, How to Complain to the NHS (Aug. 21 2021, 10:00 a.m.), https://www.nhs.uk/using-the-nhs/about-the-nhs/how-to-complain-to-the-nhs/.-

Chapter IV	*of care.*		IDs.[39] After a period of time, patients are often issued new temporary IDs, which does not maintain continuity of care.	*which personal data associated with them is collected and processed further.'*
ABHA and Other ID Policy Chapter IV	Primacy of Health ID *The absence of an Aadhaar card cannot be used to deny treatment to a patient.*	- Expressly provide for a list of documents that can be used instead of foundational identifiers in order to access benefits and prevent linkages across datasets.	Version 1.0 of the Health Data Management Policy provided for the following in its purpose: 'Voluntary use of Aadhaar per the Aadhaar Authentication for Good Governance (Social, Welfare, Innovation, Knowledge) Rules, 2020--'failure or refusal to make use of Aadhaar would not result in denial of access to any health facility or service' The 2022 version has done away with this clause, which is why an express mandate is necessary.	Linkages across multiple digital IDs creates several points of vulenrability for the data principal. Additionally, it paves the way for exclusion.

[39]Sreyan Chatterjee et. al., India's Digital Health Dreams: Getting it Right (Apr. 2022) The Dialogue, https://thedialogue.co/wp-content/uploads/2022/04/Indias-Digital-Health-Dreams.pdf.

			However, the National Digital Health Blueprint lists out the PAN, Voter Card, Ration Card among several others as different identifiers that can be used in place of Aadhaar.[40]	

[40]Ministry of Health & Family Welfare (Government of India), National Digital Health Blueprint 90 (2018).