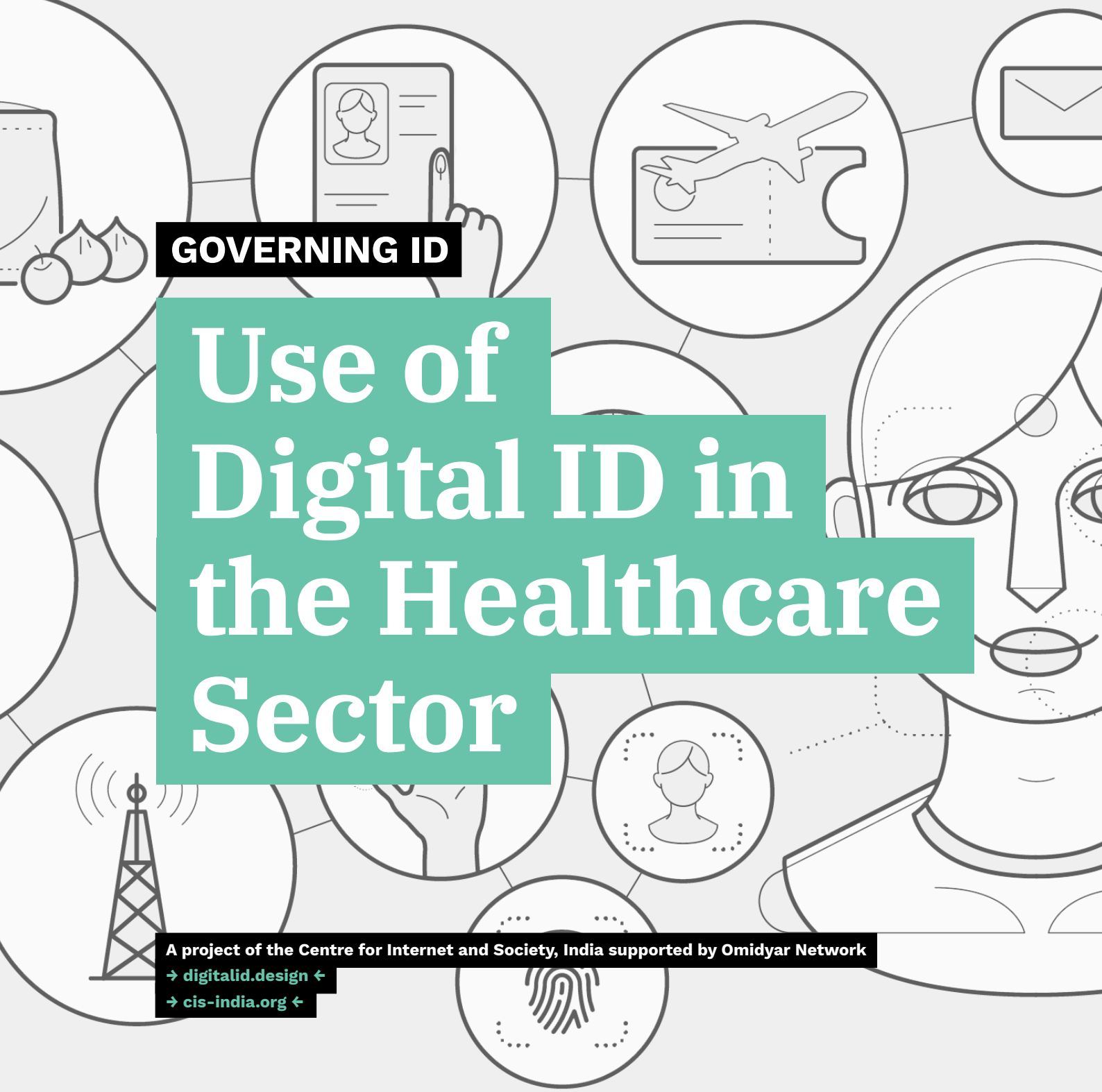

GOVERNING ID

Use of Digital ID in the Healthcare Sector

A project of the Centre for Internet and Society, India supported by Omidyar Network

→ digitalid.design ←

→ cis-india.org ←

RESEARCH & WRITING
Shruti Trikanad

REVIEW & EDITING
Amber Sinha

DESIGN
Pooja Saxena

COVER ILLUSTRATION
Akash Sheshadri

THE CENTRE FOR internet & society

INTRODUCTION

This is the third in a series of case studies, using our evaluation framework for the governance of digital identity systems. These case studies, which analyse identity programmes and their uses, illustrate how our evaluation framework may be adapted to study instances of digital identity across different regions and contexts. This case study looks at the use of digital identity programmes in the healthcare sector.

Digital IDs are being increasingly used in the healthcare industry to access patients' medical and treatment histories, and ensure consistent care. They form reliable means of identifying and authenticating patients, and allow patients to easily transfer their aggregated health records to other healthcare providers, insurance agents, etc. However, in most cases, existing foundational ID databases are leveraged to create health information databases; thus, the extension of the uses of the ID to this use also makes the ID holder, and the ID system, susceptible to a breach of sensitive personal data such as medical treatments undertaken, family medical history, etc. Here we evaluate the use of digital ID systems in the healthcare industry, across the jurisdictions of Estonia and India.

RULE OF LAW TESTS

1.1 LEGISLATIVE MANDATE

Is the use of digital identity system in healthcare codified in valid law?

The primary test to assess if digital ID is being legitimately used is whether the use is adequately codified in the law governing the issue of the ID.

In Estonia, the governing ID Act — the Identity Documents Act[1] — neither prescribes nor limits the uses of the ID; thus, the use of the digital ID in healthcare is not envisioned by the Act, but is not restricted either. The Health Services Organization Act[2] passed by the Estonian Parliament, governs the use of the ID for healthcare. It created the Health Information System, where patient data is recorded by the healthcare providers. This system leverages the digital ID in practise, though it also offers other means of identification to patients. Thus, to the extent its use is codified in *any* law, it is valid and legitimate.

Similarly, in India, the use of Aadhaar, the national digital ID, for healthcare does not form a part of the governing law, but the law leaves it open to the State to mandate its use for any other purposes. Accordingly, the National Health Stack (2018), together with the National Health Policy (2017) and the National Digital Health Blueprint Report, 2019 were issued to govern the use of the digital ID in healthcare. These policies also reference several Standards issued by the Government, including the Electronic Health Record Standard (2016), the Meity Consent Framework etc. All of these policies/Standards are issued by the Executive, and have not been considered and passed by the Parliament, and therefore cannot be considered *valid law.* Until such time they are passed as a law by the Parliament, they also contravene the Aadhaar Act which disallows Aadhaar to be mandated for any purpose unless enacted in a law passed by the Parliament.[3]

The use must be codified in valid law — the parent legislation or other supporting legislation which is in accordance with the scheme envisioned by the parent legislation. A system in which data is collected

1 Identity Documents Act, 2000.

2 Health Services Organization Act, 2002.

3 Section 6(7), The Aadhaar and Other Laws (Amendment) Act, 2019.

indiscriminately and without any purpose limitation, with its uses being determined subsequently, fails the valid law test.

1.2 LEGITIMATE AIM

Does the law have a legitimate aim?

The use of the ID must come from a legitimate aim identified in the valid law. This legitimacy must ideally correspond to a pressing social need in the population subject to the ID, and must not be limited to political expediency or enhancement of efficiency.

The Health Services Organization Act of Estonia has as its purpose the "organisation of the provision of health services," and regulating "the procedure for the management, financing and supervision of health care."[4] A majority of the governance for the use of the ID in healthcare, including in particular the collection and use of health data, is delegated to the Government of the Republic. The Statutes of Health Information System, issued by the Government, has as its purpose "the processing of health-related data for the purpose of concluding and executing a health care contract, ensuring quality of healthcare and patient's rights, protecting public health and maintaining health records, health statistics and health management."[5]

Similarly, in India, the National Health Policy lays as its objective the enhancement of efficiency and efficacy of health services, and the need to shift from a "silos system" to a holistic and comprehensive health ecosystem. The policies identified it as a problem in the current healthcare system that it was disparate and required a multiplicity of efforts from healthcare recipients.

The use of digital ID for healthcare falls under a legitimate aim.

4 Section 1(1), Health Services Organisation Act, 2002.

5 Section 2, Statutes of the Health Information System, 2016.

1.3 DEFINING PURPOSES

Does the law clearly define the purposes for which the ID can be used in healthcare?

In Estonia, although the uses are not defined in the parent ID law, it is clearly delineated in the Health Services Act read together with the Statutes of the Health Information System. The Act primarily deals with how information is collected, stored, and accessed in the information database, and to aid this it allows the data subject (or patient) to be identified by the digital ID authentication process.[6] It sets out the circumstances in which health records must be created, and how they can be accessed. Thus the governing ID framework determines purposes for its use, which are in line with the legitimate aim identified.

In India, the Health Stack, and the National Digital Health Blueprint seek to achieve their policy objectives by recommending a set of standards and APIs that can be used by private and public actors to leverage the digital health ecosystem and ensure efficiency and interoperability. It also envisions the inclusion of an insurance policy claim engine, for easy access for patients to medical insurance. In this manner, it does not prescribe specific uses of the ID, but mandates the adoption of APIs and standards that ensure the exercise of sufficient control over the ID system (or the use of the ID system). Thus, in India, the Aadhaar framework fails to clearly prescribe uses for the ID system.

For this test to be satisfied, the actors who use and control the use of ID for healthcare, must be clearly envisioned.

1.4 DEFINING ACTORS

Does the law clearly define all the actors that can use or manage the ID in healthcare?

In Estonia, the governing framework determines the actors who are required or permitted to submit data to the Health Information System are largely restricted to healthcare providers, forensic experts, and patients; and the actors that manage or control the database are the Ministry of Social Affairs as the controller

6 Section 15, Statutes of the Health Information System, 2016.

and the Health and Welfare Information Systems Center and the Estonian Healthcare Imaging Foundation as the authorized processors. However, this scope is widened by the attempt to ensure interoperability; it also requires the chief processors of the Population Register, the National Register of Health Care Professionals, the State Register of Activity Licenses for the Provision of Health Services, Prescription Centres; the Estonian Health Insurance Fund; the Estonian Unemployment Insurance Fund; and the Emergency Response Center, to submit information to the System.

The Actors who have access to the database are healthcare providers, patients, a forensic expert of a state forensic institution, officials of the Ministry of Social Affairs (for health statistics),[7] and third parties who have a "statutory right of access to data" contained in the System.[8] The data subject is also permitted to grant access to any third party provided informed consent is sought.[9] Thus, while it does specify the actors that are associated with the database, it does not restrict access of other actors, provided it is permitted by any law or by the patient themselves. This fails the test, as it allows new actors to leverage the ID system without any purpose limitation, and without sufficient governance from the ID Act.

In India, the governing framework does not specify the actors that have access to the digital ID system. However, it sets out a framework where actors seeking to access the ecosystem are registered with Master Directories, which enable "Identity and Access Management" for health apps that use the digital ID framework. This ensures the app can verify the identity of the actor attempting to use the ecosystem, and only allow access to those records that they are authorized to access.[10] Thus although it does not specify or restrict the actors that can access the system, it imposes regulatory control over it by requiring them to register with the directory, and by authorizing them to access specified data in specified circumstances. The policies, however, are unclear on exactly *who* will be managing these registries, but since existing registries of a similar nature are overseen by the Ministry of Health and Family Welfare, it is likely to be a similar Government body.

For this test to be satisfied, the actors who use and control the use of ID for healthcare, must be clearly specified through a legislative process.

7 Chapter 5, Health Services Organisation Act, 2002.

8 Section 12, Statutes of Health Information System, 2016; Section 59^3 (6), Health Services Organisation Act, 2002.

9 Section 20, Statutes of Health Information System, 2016.

10 Page 6, National Digital Health Blueprint, 2019.

1.5 REGULATING PRIVATE ACTORS

Is this use of the ID system by private actors adequately regulated?

In Estonia, the private actors that access the system are largely healthcare providers, besides those that are permitted to under any other law, or those that sought the consent of the data subject. Healthcare providers are those health care professionals who are registered with the Health Board[11] under the Act. At every instance of request for access to data in the system, the validity of the healthcare provider's activity license is checked. Thus, to that extent, there is sufficient governance over the private actors that access the database. However, private actors are also granted access rights under any other law, without any oversight mechanism established under the Healthcare Act. This fails the test, as it allows an entire set of actors to access and use the system without establishing any oversight/governance under the parent ID Act.

As for India, actors that intend to access the digital ID ecosystem are required to register with the relevant registries — Facilities, doctors, nurses and paramedics, health workers, and allied professionals have separate independent directories — and are only given access to the system based on their specific authorizations. The Policies are not currently clear on the authority imposing regulatory control over these directories, but they do indicate overarching control by a government agency. The ecosystem also creates a Health Information Exchange ("HIE"), with which every actor desiring to share or retrieve information, must be registered. The HIE is then responsible for authentication and authorization of data requests, and for channeling such data to their destination. However, apart from this, the policies seem to encourage private actors to indiscriminately leverage the system, in the form of health applications offered to customers, by adopting the API and interoperability standards. Once again, this is not in consonance with an adequate regulatory mechanism over the use of personal information by private actors.

In both cases, the use of ID for healthcare by private actors is envisioned without adequate regulation.

11 Section 27, Health Services Organisation Act, 2002.

1.6 DATA SPECIFICATION

Does the law clearly define the nature of data that will be collected?

The Health Services Organisation Act of Estonia indicates broad categories of data that must be submitted to the System, by various actors.[12] It delegates the detailing of such information to the "minster responsible for the area." [13] The Statutes of the Health Information System, issued by the Minister, mandate the submission of certain kinds of data including "information concerning the provision of in-patient healthcare" and "information for the maintenance of waiting lists" etc, without specifying the exact data that this involves, or without restricting any kinds of data.[14] It also requires healthcare providers to comply with relevant standards published by the authorized processor(s).[15] With other data providers such as the processor of the Population register and the State License Register, the categories of data to be submitted is specific and restricted.[16]

In India, the Digital Health Blueprint refers to a set of standards that must be adopted by actors uploading health records, primarily the Fast Healthcare Interoperability Resources (FHIR) R4 Specification. This Standard sets out 8 classes of *essential* and *minimum* health record artefacts that are to be collected including patient demographics and care provider details; history and diagnosis; results, assessment, vitals; adverse event and alerts; medication, lifestyle etc; procedure; admission, discharge, transfer, referral; and insurance. Thus, it does not limit the categories of data that can be collected but merely prescribes the minimum. Apart from this, the Blueprint also specifies that only *significant* medical and health episodes must be recorded, to prevent the system from being overburdened with data. However, even while mandating the maintenance of PHRs, it does not prescribe or limit the nature of data collected, and allows such determination to be done by the healthcare provider creating the PHR. Additionally, it makes no mention of principles of data minimization in the collection and processing of data; in the absence of a data protection law, this

12 Section 59^{1}, Health Services Organisation Act, 2002.

13 Section $59^{2}(2)$, Health Services Organisation Act, 2002.

14 Section 5, Statutes of Health Information System, 2016.

15 Section 5(4), Statutes of Health Information System, 2016.

16 Section 6, Statutes of Health Information System, 2016.

would have been an important measure. The ID framework fails to specify the categories of data that form part of the ID database.

The use of ID for healthcare must be accompanied by clear specification of the personal data to be collected and processed.

1.7 USER NOTIFICATION

Does the ID system provide adequate user notification mechanisms for this use case?

In Estonia, the framework does not envision notifying users when their data is being sent to the System, or when it is being accessed. This is particularly a problem in Estonia, because the ID system does not seek consent from the ID holder every time their data is being accessed. There is, however, a patient portal through which patients can access their records and determine how it has been created/ accessed and by whom.[17]

The system also fails to have a proactive notification mechanism in case of breach of the system. However, the Personal Data Protection Act, which is applicable provided contradictory obligations are not imposed through specific regulations, mandates notifications for breach of data (to the Data Protection Inspectorate and the data subject) if it is likely to entail a high risk to the rights and freedoms of natural persons, within 72 hours of becoming aware of it. It also requires that the notification include a description of the possible consequences of the personal data breach. Thus, there is a notification mechanism in place that partially fulfills this test, although the lack of a consent requirement while accessing data or creating electronic health records is alarming.

In India, the regulatory framework refers to the Electronic Health Record Standards, 2016, to ensure the privacy and reliability of personal health records. The EHR standards, in turn, provide that *general* consent must be taken from the patient or next of kin, where information is needed for "treatment, payments, and other healthcare options."[18] Though it does not go on to explain "general consent,"

17 Patient Portal, accessible at *https://m.digilugu.ee/login?locale=en*.

18 Electronic Health Standards, 2016, *https://mohfw.gov.in/sites/default/files/EMR-EHR_Standards_for_India_as_notified_by_MOHFW_2016_0.pdf.*

it has been taken to mean *implied* consent.[19] On the other hand, for non-routine and non-healthcare reasons, specific (written, express) consent is needed.[20] Finally, for national priority activities like notifiable or communicable diseases, no prior authorization is required. This acts as notification to users when their data is being accessed, but there does not seem to be a clear mechanism for when patient data is being *recorded* or *uploaded* to the EHR framework. However, it is not clear which of the principles reflected in the EHR Standards will actually be incorporated into the resulting framework, as the Blueprint merely proposes that "provisions, guidelines, and standards prescribed by the EHR STandard" be incorporated.[21]

Additionally, the Meity Electronic Consent Framework, which was determined as the appropriate standard for consent management, recommends that the consent artifact sent to the ID holder, when consent is being requested, must contain a section that *logs* consent and data flows.[22] This would include identifiers for entities that collect/store logs, thereby allowing users to easily access data about the entities accessing their personal information. It also recommends that logs could be sent to the users email address if they so desire. Additionally, it proposes that consent and data flows be properly logged and notified ("as necessary"), including information on when consent as created and when it was revoked, and when data was requested, when it was sent, and when it was denied.[23]

The policies do not identify any mechanism for notification in case of breach of the system, and in the absence of a data protection framework, there are no generally applicable obligations either that mandate such a notification (either to an authority or to the ID holder). Since the digital health framework is intended to be leveraged by private actors, there is already a disincentive to expose security

19 Omprakash Nandimath, "Consent and medical treatment: the legal paradigm in India", *Indian Journal of Urology* (2009), *https://www.google.com/url?q=https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2779959/&sa=D&ust=1578036651498000&usg=AFQjCNFeQzAPIOxMowhVe3um3YUbMb2Ccg;* The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulation, 2002,*https://ijme.in/articles/the-indian-medical-council-professional-conduct-etiquette-and-ethics-regulations-2002/?galley=html*.

20 *Id.*

21 Page 32, National Digital Health Blueprint 2019.

22 Electronic Consent Framework, Technology Specifications version 1.1, *http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf* ("Electronic Consent Framework").

23 6.2, Electronic Consent Framework.

breaches or vulnerabilities, and in the absence of obligations, this seriously impairs the safety of users' data.

There must be user notification both for use and for any data breach, while using personal data for healthcare purposes. It must be noted that healthcare data is extremely sensitive and capable of causing significant harm of the data subject.

1.8 USER RIGHTS

Do individuals have rights to access, confirmation, correction and opt out?

In Estonia, data subjects have right to confirmation and access. Section 16 of the Statutes of Health Information System, read with Section 59^3 of the Health Services Act allow the patient to access their own information. Further, patients can access the data collected about them on the Patient Portal, through their e-ID.[24] Through this portal, patients can also submit (personal) data of their own, records statements of intention, etc.

The right to modification/rectification is also largely guaranteed by the framework. The data subject has the right to modify only those personal data in the System which originate from the person's own information; they cannot modify the data entered by other actors. However, the data subject can require the controller or processor to rectify any incorrect information entered according to the procedure detailed in the GDPR.[25] The Act also allows the provider (but does not mandate) to set a time limit before forwarding data to the System so that the patient can first examine the accuracy of the personal information.

Finally, while patients may not be able to opt out of the system entirely, they have the right to prohibit access to their data by healthcare providers.[26] They can do this by making a statement of intention to the controller, processor, or the healthcare provider. Based on this, the processor of the healthcare provider must restrict access to the personal data of the patient in the System.

24 Patient Portal, accessible at *https://www.digilugu.ee/login*.

25 Section 18, Statutes of Health Information System, 2016.

26 Section $59^3(3)$, Health Services Organisation Act, 2002.

In India, patients have the right to access their own personal health records without any time restrictions. However, the healthcare provider (that created or updated the record) can deny access to such information if "in the opinion of a licensed healthcare professional the release of information would endanger the life or safety of the patients and others."[27]

In order to correct data recorded in the system, express consent of the healthcare provider that created the record or uploaded that particular data is necessary; this can also be done by a set of preferences already set by the user/manager of data.[28] This consent is not required for amending personal/demographic details in the Record, in which case the patient can do it themselves. Patients are also specifically allowed the right to demand a copy of the medical records held by a healthcare provider, which must be complied with within 30 days of the communication. They can also require the healthcare provider to withhold some information in the record that they do not want disclosed to other providers. Patients can also demand details of disclosures performed on that record.[29]

In both cases, ID holders' rights to their data are adequately guaranteed, even though they are not permitted to opt out of the system entirely. In both cases, the digital ID is not their only legal way to access the system, and thus they may be able to opt out of using their ID to access the system.

1.9 REDRESSAL MECHANISM

Are there adequate civil and criminal redressal mechanisms in place to deal with violations of their rights arising from the use in healthcare?

Supervision over the Estonian Health Information System is done by the chief controller, the Ministry of Social Affairs, the Estonian Information System's Authority, the Data Protection Inspectorate, and the Health Board.[30] The chief processor of the System is also authorized to verify compliance when the data subject intends to release their data to third parties. However, the ID framework

27 Page 21, Electronic Health Record Standards, 2016.

28 Electronic Health Record Standards, 2016.

29 Electronic Health Record Standards, 2016.

30 Section 22, Statutes of Health Information System, 2016; Section 53^1, Public Information Act, 2001.

itself sets up no redressal mechanism to regulate violations of rights arising from the collection and use of data in the Health Information System. General principles under the Personal Data Protection Act fill this gap, and the Data Protection Inspectorate acts as an extra-judicial body to settle complaints from persons whose rights have been violated under the Act.[31] Compensation may also be payable for violation of rights, under the State Liability Act[32] in case of violations by State while performing public duties, or Law of Obligations Act[33] in case of private parties in contractual relationships. Thus, while the ID system itself fails to set up an adequate mechanism, the data protection framework sufficiently addresses this gap.

In India, the Blueprint creates the National Digital Health Mission ("NDHM") to oversee the functioning of the digital health data ecosystem, and recommends that its ownership be a combination of Central and States Governments (without any private ownership). The NDHM is tasked with providing the platform for collection of healthcare data, ensuring its reliability etc. However, the specific tasks of the NDHM as a regulator/administrator are not encapsulated, and seem to be left to the wisdom of the executive when the need arises. Further, there is no mention of any redressal mechanisms, and the framework does not address any possibility of a breach or any other violation that may arise from the functioning of the system. Under the overarching Aadhaar framework, there is an Adjudicating Authority and Appellate Tribunal to deal with violations of the Act, along with a system of civil and criminal penalties; however, it is not clear how the health data framework will interact with the Aadhaar framework, as the former stores data in a federated structure and not with the Central Repository as is done with Aadhaar data). Thus, the framework governing the processing of health data is grossly inadequate to deal with violation of rights from the use of the system.

There is a need for adequate redressal mechanism whether is through the legislation governing this specific use, or through other laws such as the data protection law.

31 Section 56, Personal Data Protection Act, 2019.

32 State Liability Act, 2002, accessible at *https://www.riigiteataja.ee/akt/113092011011* [in Estonian].

33 Law of Obligations Act, 2018.

RIGHTS BASED TESTS

2.1 DATA MINIMISATION

Are principles of data minimisation followed in the collection, use, and retention of personal data for this use case?

In Estonia, while the categories of data to be collected are specified and restricted, the framework encourages interoperability and the repurposing of collected information, by requiring processors of other databases to submit data to the Health Information System without fresh consent from the ID holder. Even within the specified categories of data to be submitted, information collected includes patient's profession and employer, description of work conditions, educational institution, etc.[34] The inclusion of vast categories of non-medical data in the electronic health records, without any stated purpose, is excessive. Additionally, it requires that medical records, data about time and recipients of release of information, composition of data released etc be stored for a minimum of 30 years, with all other data not specified by legislation being stored permanently. This does not follow principles of data minimization.

As for India, by not prescribing or limiting the nature of data to be collected, the National Health Stack, and the accompanying Blueprint, do not follow principles of data minimization. Further, the applicable EHR standards require that the medical records be preserved for the lifetime of the person at least. It recommends that the status of the record be changed from active to inactive only 3 years after the death of the patient; and it never be destroyed or permanently removed.

In both cases, we see an excessive and unreasonable collection of data that flouts principles of data minimization. There should be rules in place to determine the appropriate amount of data to be collected and its retention period.

34 Annexes, Regulation on Data Content of Documents Forwarded to Health Information System and the Conditions and Arrangements for Retention of these Documents, 2008, accessible at *https://www.riigiteataja.ee/akt/112092019004* [in Estonian only].

2.2 ACCESS TO DATA

Does the law specify access that various private and public actors have to personal data in this use case?

In Estonia, the regulatory framework permits "healthcare providers," besides various State bodies, to access and submit personal information, to the Health Information System. Health care providers are defined by the Health Services Act as "health care professionals or legal persons providing health services."[35] Health care professionals are those registered with the Health Board,[36] while the Act specifies categorically the persons who may provide health services.[37] Thus, to this extent, the governing framework is specific about the access that various actors have to the system, and consistently maintain regulatory control over them.

In India, for the purposes of accessing electronic records while providing medical services, or collecting and uploading data, the framework does not differentiate between public and private actors. Actors are permitted access based on how they are authorized, depending in turn on their registration with specified registries. There are different independent registries for facilities, doctors, nurses and paramedics, health workers, and allied professionals respectively, and access is granted to individual service providers based on which registry they are registered with. Thus the framework neither specifies or limits access, nor delineates criteria on which actors may be authorized; however it does seem to propose a system in which such access will be regulated.

The Estonian use of digital ID mandates better control over access to data.

35 Section 4, Health Services Organisation Act, 2002.

36 Section 3(1), Health Services Organisation Act, 2002.

37 Section 4^3, Health Services Organisation Act, 2002.

2.3 EXCLUSIONS

Is the use of digital ID to access services exclusionary in this use case?

In Estonia, the regulatory framework allows a healthcare provider access to data in the system for "entry into and performance of a contract for the provision of a health service."[38] Thus, to this extent, it may be exclusionary for patients who cannot or do not access their digital ID. However, ID holders are also permitted to restrict access to certain data from their healthcare providers; thus, in these situations, they may be allowed access to services without sharing such restricted data.

In India, the framework does not mandate one particular ID to be used while creating a digital health identifier, and merely recommends the adoption of Aadhaar for its uniqueness and notes that in the absence of Aadhaar, the user may use a substitute national ID. However with respect to the digital health identifier itself, healthcare service providers are merely incentivised to collect and record health data; the framework does not identify penalties that will be incurred for non-compliance. Thus, the framework does not disallow the provision of services without leveraging the digital health system. However, it must also be noted that in the event that incentives are in place for healthcare providers to comply with this framework, it is likely that patients who do not or cannot partake are denied services and therefore excluded.

In order to reduce exclusionary impact, it is imperative that individuals are allowed to use other forms of ID, as well as given greater say in controlling the access to their data.

38 Section 59^3(2), Health Services Organisation Act, 2002.

RISK BASED TESTS

3.1 RISK ASSESSMENT

Is this use case regulated taking into account its potential risks?

In Estonia, the framework does not seem to have taken into account possible risks from the use of the ID. The Health Information System leverages data already collected and stored in several different databases, through mandating interoperable systems. Using the same unique ID, across multiple uses, exposes the ID system to additional risks, ones that were possibly not envisioned when the ID was first issued.

In terms of security, the EHR system is determined at the highest security level,[39] requiring independent auditing of the Estonian National Health Information System ("ENHIS") every 2 years. However, encryption of ENHIS data is not mandated by the governing law, although it is widely practised nonetheless.[40]

In India, the framework governing the use of digital ID in healthcare is not yet fully conceptualised. To the extent that it does not mandate the use of Aadhaar as an identifier, it is cognisant of risks of exclusion, and of those entailed in the linking of independent databases containing personal information. Further, the framework also proposes that a federated architecture be adopted, such that information is not all stored in a centralised database prone to security risks. However, conversely, it proposes the adoption of APIs by any service provider — with limited, not yet fully delineated regulatory control — and negligible prescription of the nature of data to be collected, where and how it will be stored, opt out mechanisms, the nature of the "trustees" who will facilitate access to data, etc.

The potential harms arising out of misuse of healthcare data are significant and therefore, the use of digital ID must be accompanied with proper risk assessment. As of now such assessment is lacking in both India and Estonia.

39 Section 91(1), Regulation on System of Security Measures for Information Systems, 2007, accessible at *https://www.riigiteataja.ee/akt/13125331* [in Estonian only] ; Section 7, Statutes of Health Information Systems, 2016.

40 Overview of the national laws on electronic health records in the EU member States, National Report for the Republic of Estonia (2014) vi.

3.2 PRIVACY RISK MITIGATION

Is there a national data protection law in place?

In Estonia, the Data Protection Act, as well as the General Data Protection Regulation, are applicable.

In India, there is not yet a national data protection law, although one is being currently considered by the Parliament.

The presence of a robust data protection framework that governs healthcare personal data adequately reduces the risks.

3.3 PRIVACY BY DESIGN

Are there privacy by design systems that minimise the harms from data breach?

No, we do not see any significant privacy by design strategies for use of digital ID is healthcare.

3.4 RESPONSE TO RISKS

Is there a mitigation strategy in place in case of failure or breach of the ID system?

No, we do not see any significant mitigation strategies to address failure of breach of the ID system when dealing with healthcare data.