RESPONSES TO THE GOVERNMENT OF INDIA'S JOINT PARLIAMENTARY COMMITTEE'S CONSULTATION ON THE PERSONAL DATA PROTECTION BILL, 2019

IMPLICATIONS on HEALTH DATA

Facilitated by:
The India Digital Health Network,
Lakshmi Mittal and Family South Asia Institute at Harvard University

Supported by:
The FXB Center for Health and Human Rights at Harvard University
The Harvard Global Health Institute Burke Fellowship

Personal Data Protection Bill: Implications on Health Data **February 2020**

The India Digital Health Network at the Lakshmi Mittal and Family South Asia Institute is an interdisciplinary faculty initiative that has contributed to policy-making and research in digital health implementation science in India. In close collaboration with colleagues from academia, industry and government, in the US and India, IDHN has submitted responses to the White Paper of the Committee of Experts on the Data Protection Framework for India; drafts of NITI Aayog's National Health Stack; and the Ministry of Health and Family Welfare's National Digital Health Blueprint; all accessible at https://mittalsouthasiainstitute.harvard.edu/india-digital-health-net/

Our responses here are once again focused on clauses that are likely to have significant impact on health data, and consequently on clinical well-being, population health and medical science. Response are submitted in-line, following the clause they refer to, highlighted in bold.

The responses recorded here are a summary of expert-opinions provided by the listed authors and are not meant to represent the position of their affiliate institutions.

Additional analysis will be published in the coming months, and any additions to this Response will be posted on the IDHN website.

We would like to especially acknowledge Nivedita Saksena, inaugural IDHN fellow at the Mittal institute for leading the review process. We are very grateful for the time, attention and counsel provided by all contributing authors.

And finally, we thank the Joint Parliamentary Committee on the Personal Data Protection Bill for this opportunity to respond to the Bill.

Sincerely,
On behalf of the contributing authors,

Satchit Balsari, MD, MPH

Assistant Professor, Emergency Medicine, Harvard Medical School
Assistant Professor, Global Health and Population,
Harvard TH Chan School of Public Health

The India Digital Health Network,
Lakshmi Mittal and Family South Asia Institute at Harvard University

Who knows? Who decides? Who decides who decides?

- Shoshana Zuboff, in *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*

CONTRIBUTORS

Dr. Abhijeet Waghmare	St. John's Research Institute
Dr. Adrian Gropper	Patient Privacy Rights
Angshuman Sarkar	ThoughtWorks
AV Sethuraman	Argusoft
Clay Heaton	FXB Centre for Health and Human Rights
Dr. Geetika Sethi	Scientist ICMR-AIIMS Computational Genomics Centre
Dr. Guriqbal Singh Jaiya	Honorary Advisor ICMR-AIIMS Computational Genomics Centre
Dr. Harpreet Singh	Scientist and Head ICMR-AIIMS Computational Genomics Centre
Jimmy Anthony	St. John's Research Institute
Nivedita Saksena	India Digital Health Network Fellow Lakshmi Mittal South Asia Institute at Harvard
Rahul Matthan	Trilegal
Dr. Satchit Balsari	Harvard Medical School Burke Fellow, Harvard Global Health Institute
Dr. Shrey Desai	SEWA Rural
Sneha Vaidhyam	St. John's Research Institute
Supten Sarbadhikari	Independent Consultant
Tarun Khanna	Harvard Business School
Dr. Tony Raj	St. John's Research Institute

AS INTRODUCED IN LOK SABHA

Bill No. 373 of 2019

THE PERSONAL DATA PROTECTION BILL, 2019

A

BILL

to provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organisational and technical measures in processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data, remedies for unauthorised and harmful processing, and to establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto.

WHEREAS the right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy;

AND WHEREAS the growth of the digital economy has expanded the use of data as a critical means of communication between persons;

AND WHEREAS it is necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation through digital governance and inclusion and for matters connected therewith or incidental thereto.

BE it enacted by Parliament in the Seventieth Year of the Republic of India as follows:—

READING KEY:
Bold text: Clauses we have responded to
Regular text: our responses
Grey text: Clauses we have not responded to

CHAPTER I

PRELIMINARY

1. (*1*) This Act may be called the Personal Data Protection Act, 2019.

(*2*) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint; and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision.

2. The provisions of this Act,— (*A*) shall apply to—

(*a*) the processing of personal data where such data has been collected, disclosed, shared or otherwise processed within the territory of India;

(*b*) the processing of personal data by the State, any Indian company, any citizen of India or any person or body of persons incorporated or created under Indian law;

Replace the term "citizen" with "resident." In healthcare, this clause, as it is written, would apply to data of patients being processed by non-resident Indian physicians practicing overseas.

(*c*) the processing of personal data by data fiduciaries or data processors not present within the territory of India, if such processing is—

(*i*) in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India; or

(*ii*) in connection with any activity which involves profiling of data principals within the territory of India.

(*B*) shall not apply to the processing of anonymised data, other than the anonymised data referred to in section 91.

3. In this Act, unless the context otherwise requires,—

(*1*) "Adjudicating Officer" means the Adjudicating Officer appointed as such under sub-section (*1*) of section 62;

(*2*) "anonymisation " in relation to personal data, means such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Authority;

Anonymized data should not completely be out of the purview of this bill. Every anonymized data risks re-identification when combined with other datasets. Data fiduciaries should therefore be expected to show restraint (through time and purpose limitation) even when data are anonymized.

Conversely, the value of data in medicine is often in its high resolution. As the world advances toward precision medicine, techniques to de-identify, aggregate and anonymize data rid the data of the rich granularity required to conduct robust, statistically valid experiments. Data archiving, retrieval and exchange modalities at research institutions are often outmoded and not in sync with technological advances, putting at risk the privacy of data principals. But the only solution there is not to anonymize the data and make them unusable for many scientific applications. The requirements on anonymization should be treated differently when dealing with health data, because both the risks to and the potential benefits from such data are very high.

(*3*) "anonymised data" means data which has undergone the process of anonymisation;

This Bill should spell out what anonymization means, or at least provide a working definition. It would be important to mention that the assumption that the anonymization protects against re-identification is tenuous.

(*4*) "Appellate Tribunal" means the Tribunal established under sub-section (*1*) or notified under sub-section (*4*) of section 67;

(*5*) "Authority" means the Data Protection Authority of India established under sub-section (*1*) of section 41;

(*6*) "automated means" means any equipment capable of operating automatically in response to instructions given for the purpose of processing data;

Consider replacing the word “equipment” with “hardware or software” or “machine or program”

(*7*) "biometric data" means facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological, or behavioural characteristics of a data principal, which allow or confirm the unique identification of that natural person;

Consider including the term digital phenotyping as well. How people interact with their phones (how they hold them, were they touch the screen, the tremor in their hands, how often they use the use it, and for what purpose, all constitute information that can be collated to create a unique digital identity for a person; and with evolving technology, wearable devices may also be able to identify person based on how, where and when the move.

Such information is already being used to build algorithms to detect medical conditions like "tremors," or predict mental health of individuals, and is likely to be increasingly used to study the effect of and compliance with medical interventions (including pharmaceuticals, behavioral therapies, and surgical interventions).

We recommend the following revised definition for biometric data under clause 3(7):

Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, such as facial images, fingerprints, iris patterns, retina patterns, palm vein patterns, and shapes of the ear, footprint features, signatures, hand geometry or any other similar personal data which allow or confirm the unique identification of that natural person.

(*8*) "child" means a person who has not completed eighteen years of age;

(*9*) "code of practice" means a code of practice issued by the Authority under section 50;

(*10*) "consent" means the consent referred to in section 11;

(*11*) "data" includes a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means;

(*12*) "data auditor" means an independent data auditor referred to in section 29;

(*13*) "data fiduciary" means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data;

Sector specific definitions will be important. It may be helpful to establish a hierarchy of obligations on data fiduciaries. The more data (in volume and diversity) the data fiduciary has, the more stringent its obligations may have to be.

For example, a bank is a fiduciary with no expectation of aggregation of outside data. A credit card or payment processor has more information from more sources still under the control of the data principal. A credit bureau aggregates personal information from numerous sources and the data principal has some control but not much. Finally, a government agency may have even more data from more sources about a data principal and the existence of that dossier is often secret or hidden from the principal. These four roles are very different.

Similarly, a national chain of laboratories may franchise its operations to local labs. In this contest the local labs are data processors, the national chain a data fiduciary, but not an account aggregator. But the Personal Health Record service, or an Electronic Health Record product that draws patients' data from the laboratory and from other services like hospitals and chemists, would constitute an account aggregator - as would, an insurance agency that would also have access to such data.

For the sections below,
Consider first introducing the "data principal," then the processor, and so on up the chain.
Consider including here the definition of "significant data fiduciary" as well.

(*14*) "data principal" means the natural person to whom the personal data relates;

(*15*) "data processor" means any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary;

(*16*) "de-identification" means the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal;

(*17*) "disaster" shall have the same meaning as assigned to it in clause (*d*) of section 2 of the Disaster Management Act, 2005;

(*18*) "financial data" means any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history;

(*19*) "genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the behavioural characteristics, physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

Please note: “genetic data” relates not just to the natural person, but also carries information about other natural persons to varying degrees. This definition should be modified.

(*20*) "harm" includes—

(*i*) bodily or mental injury;

(*ii*) loss, distortion or theft of identity;

(*iii*) financial loss or loss of property;

(*iv*) loss of reputation or humiliation;

(*v*) loss of employment;

(*vi*) any discriminatory treatment;

(*vii*) any subjection to blackmail or extortion;

(*viii*) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal;

(*ix*) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or

(*x*) any observation or surveillance that is not reasonably expected by the data principal;

(21) "health data" means the data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, data associating the data principal to the provision of specific health services;

Note here that emerging technologies are generating data that may not intuitively have been considered “health data,” but do have predictive power with regards to human health. For example, data from the gyroscopes and accelerometers in our phones, as well as location data, may reliably predict a sedentary versus active lifestyle, mobility, mental health and gait stability. By stating that “"health data" means the data related to the state of physical or

mental health of the data principal," the language of this Bill may have impact on other laws that define the scope of, and regulate medical devices.

(22) "intra-group schemes" means the schemes approved by the Authority under clause (*a*) of sub-section (*1*) of section 34;

(23) "in writing" includes any communication in electronic format as defined in clause (r) of sub-section (1) of section 2 of the Information Technology Act, 2000;

(24) "journalistic purpose" means any activity intended towards the dissemination through print, electronic or any other media of factual reports, analysis, opinions, views or documentaries regarding—
(*i*) news, recent or current events; or
(*ii*) any other information which the data fiduciary believes the public, or any significantly discernible class of the public, to have an interest in;

(25) "notification" means a notification published in the Official Gazette and the expression "notify" shall be construed accordingly;

(26) "official identifier" means any number, code, or other identifier, assigned to a data principal under a law made by Parliament or any State Legislature which may be used for the purpose of verifying the identity of a data principal;

(*27*) "person" includes—

(*i*) an individual,
(*ii*) a Hindu undivided family,
(*iii*) a company,
(*iv*) a firm,
(*v*) an association of persons or a body of individuals, whether incorporated or not,
(*vi*) the State, and
(*vii*) every artificial juridical person, not falling within any of the preceding sub-clauses;

How will this definition include (or exclude) persons that are dead or entities that have gone out of business? What rights (and obligations) will such entities or persons have ?

(*28*) "personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling;

By this definition, anonymized data fall under the purview of this Bill, as anonymized data also run the risk of being re-identifiable when combined with other datasets, depending on the content and availability of those other datasets.

(*29*) "personal data breach" means any unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to, personal data that compromises the confidentiality, integrity or availability of personal data to a data principal;

(*30*) "prescribed" means prescribed by rules made under this Act;

(*31*) "processing" in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;

Consider introducing the terms “purposeful or inadvertent,” to include hacking, and other illegitimate uses of data.

(32) "profiling" means any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a data principal;

(33) "regulations" means the regulations made by the Authority under this Act;

(34) "re-identification" means the process by which a data fiduciary or data processor may reverse a process of de-identification;

(35) "Schedule" means the Schedule appended to this Act;

(36) "sensitive personal data" means such personal data, which may, reveal, be related to, or constitute—

(i) financial data;
(ii) health data;
(iii) official identifier;
(iv) sex life;
(v) sexual orientation;

(vi) biometric data;
(vii) genetic data;
(viii) transgender status;
(ix) intersex status;
(x) caste or tribe;
(xi) religious or political belief or affiliation; or
(xii) any other data categorised as sensitive personal data under section 15.

Explanation.— For the purposes of this clause, the expressions,—

(a) "intersex status" means the condition of a data principal who is—

(i) a combination of female or male;
(ii) neither wholly female nor wholly male; or
(iii) neither female nor male;

(b) "transgender status" means the condition of a data principal whose sense of gender does not match with the gender assigned to that data principal at birth, whether or not they have undergone sex reassignment surgery, hormone therapy, laser therapy, or any other similar medical procedure;

It must be clarified here how personal data that reveals caste or tribe status is defined. For instance, does this include all surnames? It may also be possible to link this definition to the definition under the Constitution and the Scheduled Caste/Scheduled Tribes (Prevention of Atrocities) Act.

(37) "significant data fiduciary" means a data fiduciary classified as such under sub-section (1) of section 26;

(38) "significant harm" means harm that has an aggravated effect having regard to the nature of the personal data being processed, the impact, continuity, persistence or irreversibility of the harm;

(39) "State" means the State as defined under article 12 of the Constitution;

(40) "systematic activity" means any structured or organised activity that involves an element of planning, method, continuity or persistence.

CHAPTER II

OBLIGATIONS OF DATA FIDUCIARY

4. No personal data shall be processed by any person, except for any specific, clear and lawful purpose.

5. Every person processing personal data of a data principal shall process such personal data—

(a) in a fair and reasonable manner and ensure the privacy of the data principal; and

(*b*) for the purpose consented to by the data principal or which is incidental to or connected with such purpose, and which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected.

There will need to be further sector-specific elaboration of what is "reasonable," and "incidental." These terms are problematic, as illustrated in the examples below:

For example, it is reasonable to expect that health data may be generated, collected, stored, and transmitted by a clinical establishment and; collected, stored and transmitted by health information exchange, for the following purposes:
(a) Given back in summary form, report or prescription at the completion of an encounter with the health provider
(b) To advance the delivery of patient centered medical care;
(c) To provide appropriate information to help guide medical decisions at the time and place of treatment;
(d) To improve the coordination of care and information among hospitals, laboratories, medical professionals, and other entities through an effective infrastructure for the secure and authorized exchange of digital health data;
(e) To improve public health activities and facilitate the early identification and rapid response to public health threats and emergencies, including bioterror events and infectious disease outbreaks;
(f) To facilitate health and clinical research and health care quality;
(g) To promote early detection, prevention, and management of chronic diseases;
(h) To carry out public health research, review and analysis, and policy formulation;
(i) To undertake academic research and other related purposes.

But what if the state wants to use aggregated cell-phone data to forecast or model epidemics by studying population mobility? Data principals may not have "reasonably

expected," such secondary use of their data. Should such use of data require the use of a regulatory sandbox, as prescribed below, before it is approved? One may argue that these data are aggregated and not within the purview of the Bill (we disagree).

What if the state now wants to use cellphone-based location to do contact tracing, to notify individuals that they may have been exposed to a communicable disease? While this may not be a "reasonable" expectation of secondary use, it may be considered acceptable. Every such exception must be subject to review, or be permitted by sector specific regulation and oversight.

Imagine patients downloading a diabetes lifestyle management app from the Google play store. From the perspective of the app company, in this example, it's both incidental and reasonable to collect in-app behavior metrics, and to show targeted advertising (for company financial health) when somebody tacitly consents to using the app by downloading it from an app store. Even if the app developer does not engage in those activities, the Google Play store may engage with them in an incidental manner through terms governed by Google itself (and the use of the Google Play store or a Google-distributed version of Android). This is a complex issue because Google and Android have become so prevalent that they can, in many senses, be considered utilities. It puts an undue burden on people who want to purchase a mobile phone to seek a non-Android device that is affordable, and that will not collect their data.

6. The personal data shall be collected only to the extent that is necessary for the purposes of processing of such personal data.

Please consider revising this sentence. Is this referring to data minimization? Or is it limiting secondary use of data? The latter will have detrimental effect on clinical medicine, population health research and medical research in general without additional clarification.

7. (*1*) Every data fiduciary shall give to the data principal a notice, at the time of collection of the personal data, or if the data is not collected from the data principal, as soon as reasonably practicable, containing the following information, namely:—

Clarification requested:
What will be the expectations for continuous data streams, from mobile devices and wearables?

Comment:
The term “reasonably practical” is ambiguous, and may have very different implications on data fiduciaries depending on resources available to them.

Revision recommended:
Replace the phrase ‘not collected from the data principal’ by ‘collected from a third party’

(*b*) the nature and categories of personal data being collected;

These categories should be listed under regulations or a suggested format/template provided for this notice.

(c) the identity and contact details of the data fiduciary and the contact details of the data protection officer, if applicable; and (d) the right of the data principal to withdraw consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent;

Consider requiring reciprocal ease for withdrawing consent as it is for a data principal to give consent, through a consent manager interface. The publication of the identity and contact details suggest an onerous pathway to withdrawing consent, and should only be required for redressal, and not for routine withdrawal of consent. For the most part, patients should be able to easily control what sections of their current and past medical history may be accessible to various data fiduciaries (or data processors).

If a patient changes hospitals or physicians, she may choose to withhold access to her data from her previous caregivers.

(e) the basis for such processing, and the consequences of the failure to provide such personal data, if the processing of the personal data is based on the grounds specified in sections 12 to 14;

Clarification requested: What does “basis for processing” mean? If it means “purpose,” in healthcare, it may not be possible to predict what such data may be used for in the future.

(f) the source of such collection, if the personal data is not collected from the data principal;

(g) the individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable;

(h) information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable;

It is suggested that the above may be modified as follows:

"information regarding any likelihood of or actual cross-border processing of the personal data that the data fiduciary intends to carry out, if applicable;"

(i) the period for which the personal data shall be retained in terms of section 9 or where such period is not known, the criteria for determining such period;

(j) the existence of and procedure for the exercise of rights mentioned in Chapter V and any related contact details for the same;

(k) the procedure for grievance redressal under section 32;

(l) the existence of a right to file complaints to the Authority;

(m) where applicable, any rating in the form of a data trust score that may be assigned to the data fiduciary under sub-section (5) of section 29; and

(n) any other information as may be specified by the regulations.

(*2*) The notice referred to in sub-section (*1*) shall be clear, concise and easily comprehensible to a reasonable person and in multiple languages where necessary and practicable.

Revised sub-clause 7.(2):
"The notice referred to in sub-section (1) shall be clear, concise, accessible, visible and easily comprehensible to a lay person and in multiple languages where necessary and practicable."

(*3*) The provisions of sub-section (*1*) shall not apply where such notice substantially prejudices the purpose of processing of personal data under section 12.

8. (*1*) The data fiduciary shall take necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed.

(2) While taking any steps under sub-section (1), the data fiduciary shall have regard to whether the personal data—

(a) is likely to be used to make a decision about the data principal;
(b) is likely to be disclosed to other individuals or entities including other data fiduciaries or processors; or
(c) is kept in a form that distinguishes personal data based on facts from personal data based on opinions or personal assessments.

(3) Where personal data is disclosed to any other individual or entity, including other data fiduciary or processor, and the data fiduciary finds that such data does not comply with the requirement of sub-section (1), the data fiduciary shall take reasonable steps to notify such individual or entity of this fact.

9. (*1*) The data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing.

Consider stipulating specific timelines for various types of data. Some health data need to be maintained for the lifetime of a patient (for example, the patient's allergy or significant medical history). Some data, may not be vital, for example, the history of a remote sprain. Which entity is required to maintain what data, and for how long, may be best left to specific regulations that determine how long laboratories, hospitals, and chemists, for example, may be asked to retain digital records of patient's data, and who would bear these costs. The federated architecture envisioned in the National Digital Health Blueprint released by the MoHFW puts significant obligations on health data fiduciaries to not only retain data, but make much of it easily accessible, remotely and in near real-time.

The clause as it is currently written does not differentiate between data processors, account aggregators, consent managers and data fiduciaries and may need to apply differentially to each of them.

(*2*) Notwithstanding anything contained in sub-section (*1*), the personal data may be retained for a longer period if explicitly consented to by the data principal, or necessary to comply with any obligation under any law for the time being in force.

We recommend sector specific modification of clause 9(2) that may permit data that may be considered health data, including biometric and genetic data, to be retained for the lifetime of the data principal, when necessary for provision of health services, and even longer, if permitted by regulation or consent, for research and development, innovation, archiving in the public interest, epidemiological purposes or statistical purposes in accordance with section 38 and any other purposes as may be prescribed by regulations.

(*3*) The data fiduciary shall undertake periodic review to determine whether it is necessary to retain the personal data in its possession.

(*4*) Where it is not necessary for personal data to be retained by the data fiduciary under sub-section (1) or sub-section (2), then, such personal data shall be deleted in such manner as may be specified by regulations.

10. The data fiduciary shall be responsible for complying with the provisions of this Act in respect of any processing undertaken by it or on its behalf.

11. (*1*) The personal data shall not be processed, except on the consent given by the data principal at the commencement of its processing.

We raise two issues here that are relevant to most clauses in this Bill:

Please include provisions here for those that may **not be able to give consent due to physical or mental incapacity,** but where the processing of data is necessary for the provision of medical services.

How will data of the deceased be handled?

(2) The consent of the data principal shall not be valid, unless such consent is—

(a) free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872;
(b) informed, having regard to whether the data principal has been provided with the information required under section 7;
(c) specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose of processing;
(d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and
(e) capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.

(*3*) In addition to the provisions contained in sub-section (*2*), the consent of the data principal in respect of processing of any sensitive personal data shall be explicitly obtained—

(*a*) after informing him the purpose of, or operation in, processing which is likely to cause significant harm to the data principal;

(*b*) in clear terms without recourse to inference from conduct in a context; and

(*c*) after giving him the choice of separately consenting to the purposes of, operations in, the use of different categories of, sensitive personal data relevant to processing.

(*4*) The provision of any goods or services or the quality thereof, or the performance of any contract, or the enjoyment of any legal right or claim, shall not be made conditional on the consent to the processing of any personal data not necessary for that purpose.

(*5*) The burden of proof that the consent has been given by the data principal for processing of the personal data under this section shall be on the data fiduciary.

(*6*) Where the data principal withdraws his consent from the processing of any personal data without any valid reason, all legal consequences for the effects of such withdrawal shall be borne by such data principal.

Consent should always be coercion free, and patients should not be required to provide explanation for withdrawal of consent. This clause seems to go against the spirit of free and informed consent. Consider deleting this sub-clause.

CHAPTER III

GROUNDS FOR PROCESSING OF PERSONAL DATA WITHOUT CONSENT

12. Notwithstanding anything contained in section 11, the personal data may be processed if such processing is necessary,—
(*a*) for the performance of any function of the State authorised by law for—

(*i*) the provision of any service or benefit to the data principal from the State ; or

The provision of service or benefit should not preclude the state from the obligations under this Bill. This exception precludes the necessity to have strict role-based access to healthcare data as an increasingly larger amount of health data becomes digitized and remotely accessible. Currently, it is possible for several layers of healthcare administrators to access line-level data of beneficiaries. This mindset is highly flawed, and persons not required in the direct provision of clinical care to patients, should not have access to patients' identities, as they currently do, in many circumstances.

This clause would allow, for example, the state to know which persons are receiving contraceptives from the state, or receiving treatment for tuberculosis or HIV. It is important to introduce role based access. One type of data fiduciaries, in this case, the state's department of public health, need not know the identities of the beneficiaries, but may be allowed access to aggregated data. If they were interested in knowing about spatial clustering, they may be provided such data, as long as GPS locations did not reveal the identity of the recipients. Another type of data fiduciary, the account aggregator of the patient's personal health record, may have access to sensitive personal information, but privacy by design, should ensure that no natural person working at the account aggregator can access identifying information.

A data processor, say a worker of the state, delivering HIV medications to patients's homes, will know the identity of the patients, but must be under the data protection obligations placed by this law to not reveal the identity to others including to her supervisors.

It is therefore important to have unambiguous sector-specific rules about what access is considered "necessary for processing."

(*ii*) the issuance of any certification, licence or permit for any action or activity of the data principal by the State;

It is unclear why such issuance would not require compliance with the obligations of this bill. The physician's license to practice medicine, for example, should not require the state to collect any data about the physician without her consent. In addition, the denial of such license, should require the state to be transparent about the data it based its decisions on, and must be under the same fidicuciary obligations of notice and transparency as stipulated above, to prevent discrimination, on any grounds.

(*b*) under any law for the time being in force made by the Parliament or any State Legislature; or

(*c*) for compliance with any order or judgment of any Court or Tribunal in India;

(*d*) to respond to any medical emergency involving a threat to the life or a severe threat to the health of the data principal or any other individual ;

It is important to have sector specific regulations here.

An infectious disease outbreak, for example, may allow the state to take the position that GPS-location data may be accessed to conduct contact tracing. Who decides whether such use is legitimate and for how long, and how and when these data will be destroyed? If not already permitted under sector-specific regulation, such novel uses of data may be appropriate for consideration under Regulatory Sandboxes - but a blanket exception is not advisable.

While this clause may be written for "break the glass," scenarios for critical emergencies in hospitals (trauma patient, obtunded patient, etc.), the provision that obligations may be waived for the protection of "any other individual" is ambiguous, and allows the possibility of indiscriminate use of personal data.

There is a difference between emergent care, and inability to consent, and this nuance should be addressed. This clause is best restricted to scenarios where consent may be waived when it cannot be obtained, and the delay of care threatens the wellbeing of the patient.

Consider revising:
-to respond to a severe threat to the life or a significant threat to the quality of life of a person, when consent cannot be obtained from the patient or her legal representative in a time-sensitive manner.

Further, the phrase 'medical emergency' must be defined. We recommend the following definition:

Medical emergency is the sudden onset of a medical condition *in a natural person* which in the absence of immediate medical attention could reasonably be expected to result in harm in the form of

(i) serious jeopardy to the mental or physical health of the individual,

(ii) danger of serious impairment of the individual's bodily functions,

(iii) serious dysfunction of any of the individual's bodily organs, or

(iv) in the case of a pregnant woman, serious jeopardy to the health of the fetus.

(*e*) to undertake any measure to provide medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health; or

Clarification requested: Please elaborate on the implications of cross-border data transfer, since disease surveillance data are most useful when integrated with the international health monitoring and research ecosystem.

Data fiduciaries, if allowed to waive consent for such emergencies, must be required to notify persons (even if through public dissemination), and be transparent about the type of data they will be collecting, for what purpose, and for how long. Consent may conceivably waived, but not without notice. The DPA (or other agency) should be authorized to review the validity of such exceptions, even if post-hoc; or be provided the resources to permit emergency review and authorization.

We propose the inclusion of a definition of public health emergency as follows:
Public health emergencies are situations whose health consequences have the potential to overwhelm routine community capabilities to address them. It focuses on situations whose scale, timing, or unpredictability threatens to overwhelm routine capabilities.

(*f*) to undertake any measure to ensure safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order.

The provision that the state be allowed to collect data for breakdown in public order is ambiguous, and should once again, require notice and transparency of what data it intends to collect, why and for how long. This clause is ambiguous and risks permitting mass surveillance under the guise of public health and law and order. We recommend that safeguards be introduced through reporting requirements after a disaster or 'breakdown in public order' to ensure transparency and accountability of state actors. This may include a report to be presented to the Data Protection Authority on the amount and nature of data collected, and the uses to which it was put. This report must be mandatorily available in the

public domain. The Data Protection Authority may also appoint a data auditor for this purpose.

13. (*1*) Notwithstanding anything contained in section 11 and subject to sub-section (*2*), any personal data, not being any sensitive personal data, may be processed, if such processing is necessary for—

(*a*) recruitment or termination of employment of a data principal by the data fiduciary;

Such processing may be done under a contractual obligation with notice and transparency.

(*b*) provision of any service to, or benefit sought by, the data principal who is an employee of the data fiduciary;

It is once again important to enforce role-based access. If a hospital employee is seeking care at the hospital she works at, the data fiduciary's access to her personal data should be harder, not easier, and be strictly role based. Consider the example of financial assistants at hospitals that facilitate insurance claims, who have relatively unbridled access (even if inadvertent) to personal data about the patients seeking to file their claims. "Privacy be design" should make available dashboards, for example, that provide role-based access such that only the personal data absolutely necessary for the filing of the claims, be accessible to said facilitators.

Recommendation:
Data fiduciary is obligated to ensure that access to personal data of the data principal be strictly limited to the articulated purpose of processing such data, and be restricted to as few a pool of employees as absolutely necessary, when the data principal is an employee of the data fiduciary.

(*c*) verifying the attendance of the data principal who is an employee of the data fiduciary; or
(*d*) any other activity relating to the assessment of the performance of the data principal who is an employee of the data fiduciary.

These provisions (c and d) should be covered under the contractual terms of employment, and not be provided exceptions under this Bill.

(*2*) Any personal data, not being sensitive personal data, may be processed under sub-section (*1*), where the consent of the data principal is not appropriate having regard to the employment relationship between the data fiduciary and the data principal, or would involve a disproportionate effort on the part of the data fiduciary due to the nature of the processing under the said sub-section.

This clause is unclear. As stated earlier, additional burden must be placed on data fiduciaries while processing data of employees, unless for tasks related to employment. In the latter case, consent should be obtained (not waived) at employment.

14. (*1*) In addition to the grounds referred to under sections 12 and 13, the personal data may be processed without obtaining consent under section 11, if such processing is necessary for such reasonable purposes as may be specified by regulations, after taking into consideration—

(*a*) the interest of the data fiduciary in processing for that purpose;

This would allow health care enterprises, insurance companies and individual providers to practice discrimination. Experts have argued that a "fiduciary" framework fails for precisely this reason - corporations have obligations to their stakeholders, and cannot also be expected to act in the best interest of their clients. Denial of insurance claims (or even coverage) is a well known example. Data fiduciaries, in this case, insurance companies, may choose to collect personal data about their enrollees from fitness centers, hospitals, wearable devices, and grocery stores, to determine what insurance premium to charge patients, as would be in the interest of the data fiduciaries.

(*b*) whether the data fiduciary can reasonably be expected to obtain the consent of the data principal;

The term "reasonably" is ambiguous and allows data fiduciaries to abrogate from their responsibilities.

(*c*) any public interest in processing for that purpose;

This needs sector specific regulations, and should require case-by-case review as suggested above.

(*d*) the effect of the processing activity on the rights of the data principal; and

(*e*) the reasonable expectations of the data principal having regard to the context of the processing.

(*2*) For the purpose of sub-section (*1*), the expression "reasonable purposes" may include—

(*a*) prevention and detection of any unlawful activity including fraud;
(*b*) whistle blowing;

(*c*) mergers and acquisitions;
(*d*) network and information security;
(*e*) credit scoring;
(*f*) recovery of debt;
(*g*) processing of publicly available personal data; and
(*h*) the operation of search engines.

The processing of publicly available personal data when combined with anonymized data risks re-identification of anonymized data as amply demonstrated in the literature now. So the processing of publicly available personal data should not be outside of the purview of this law. The impact of said processing of publicly available data on data principals should determine its legitimacy or permissibility.

Clarification requested:
Search Engines do not need to collect personal data without the obligations placed on data fiduciaries. Why are search engines included here?

(*3*) Where the Authority specifies a reasonable purpose under sub-section (*1*), it shall—

(*a*) lay down, by regulations, such safeguards as may be appropriate to ensure the protection of the rights of data principals; and
(*b*) determine where the provision of notice under section 7 shall apply or not apply having regard to the fact whether such provision shall substantially prejudice the relevant reasonable purpose.

15. (*1*) The Central Government shall, in consultation with the Authority and the sectoral regulator concerned, notify such categories of personal data as "sensitive personal data", having regard to—

(*a*) the risk of significant harm that may be caused to the data principal by the processing of such category of personal data;
(*b*) the expectation of confidentiality attached to such category of personal data;
(*c*) whether a significantly discernible class of data principals may suffer significant harm from the processing of such category of personal data; and
(*d*) the adequacy of protection afforded by ordinary provisions applicable to personal data.

(*2*) The Authority may specify, by regulations, the additional safeguards or restrictions for the purposes of repeated, continuous or systematic collection of sensitive personal data for profiling of such personal data.

CHAPTER IV

PERSONAL DATA AND SENSITIVE PERSONAL DATA OF CHILDREN

16. (*1*) Every data fiduciary shall process personal data of a child in such manner that protects the rights of, and is in the best interests of, the child.

(*2*) The data fiduciary shall, before processing of any personal data of a child, verify his age and obtain the consent of his parent or guardian, in such manner as may be specified by regulations .

Clarification requested: does this clause should only apply to data fiduciaries and not data processors?

The requirement for parental permission can be problematic where healthdata is concerned and have unintended or harmful consequences for teenagers less than 18 years of age seeking sexual health services, perinatal care or termination of pregnancies. A requirement that consent be sought from parents will encourage them to seek care with unlicensed providers, or worse, not seek care at all.

Special mention must also be made of emancipated minors, orphans, migrant children, street children, child laborers, refugee children, many of whom may not have access to parents or legal guardians.

(*3*) The manner for verification of the age of child under sub-section (*2*) shall be specified by regulations, taking into consideration—

(*a*) the volume of personal data processed;

(*b*) the proportion of such personal data likely to be that of child;

(*c*) possibility of harm to child arising out of processing of personal data; and

(*d*) such other factors as may be prescribed.

(*4*) The Authority shall, by regulations, classify any data fiduciary, as guardian data fiduciary, who—

(*a*) operate commercial websites or online services directed at children ; or

This has been a significant loophole under GDPR for mobile games (see footnote below), and may have similar implications in healthcare. “Services directed at children,” is ambiguous. Will it, for example, include companies that are marketing contraceptives? Does this play an undue burden on corporations?

Conversely, if a company does not state that it targets children, but the teenager buys contraception on its website, and the company collects information about the teenager, and sends more marketing material to the teenager's home, can the company state that it did know the age of the child, and therefore not be held responsible for risking her privacy?

Consider the example of mobile games under COPPA (the Californian Privacy law) and GDPR. The mobile game Subway Surfers is considered to target children because of the cartoony appearance of the characters in the game. Temple Run is not considered to target children because of the realistic appearance of the characters in the game. This is entirely subjective. The Google Play Store and iOS App Store ratings for children are out of alignment and cause additional confusion. Is it enough for Subway Surfers to state in their privacy policy "this is not intended for children and should only be played by children under the age of 18 with parental consent?"

(*5*) The guardian data fiduciary shall be barred from profiling, tracking or behavioural monitoring of, or targeted advertising directed at, children and undertaking any other processing of personal data that can cause significant harm to the child.

(*6*) The provisions of sub-section (*5*) shall apply in such modified form to the data fiduciary offering counselling or child protection services to a child, as the Authority may by regulations specify.

(*7*) A guardian data fiduciary providing exclusive counselling or child protection services to a child shall not require to obtain the consent of parent or guardian of the child under sub-section (*2*).

***Explanation.*—For the purposes of this section, the expression "guardian data fiduciary" means any data fiduciary classified as a guardian data fiduciary under sub-section (*4*).**

Consider two other special provisions, as has been done for the case of children: one for the deceased, and the other for those that cannot provide consent due to physical or mental impairment.

CHAPTER V

RIGHTS OF DATA PRINCIPAL

17. (*1*) The data principal shall have the right to obtain from the data fiduciary—

In healthcare, such access may need to be given to the legal health care proxy or surrogate. Consider rephrasing, "the data principal, or surrogate as may be prescribed by regulations,"

(a) confirmation whether the data fiduciary is processing or has processed personal data of the data principal;
(b) the personal data of the data principal being processed or that has been processed by the data fiduciary, or any summary thereof;
(c) a brief summary of processing activities undertaken by the data fiduciary with respect to the personal data of the data principal, including any information provided in the notice under section 7 in relation to such processing.

17. (*2*) The data fiduciary shall provide the information under sub-section (*1*) to the data principal in a clear and concise manner that is easily comprehensible to a reasonable person.

Consider deleting "reasonable" from the phrase reasonable person, and saying the "lay person."

(*3*) The data principal shall have the right to access in one place the identities of the data fiduciaries with whom his personal data has been shared by any data fiduciary together with the categories of personal data shared with them, in such manner as may be specified by regulations.

This is not enforceable. As the clause currently reads, any natural person should be able to log into one portal (assuming that is what is meant by "one place") to know about the whereabouts of their personal data in the entire universe, across all sectors, public, private, domestic, international, encompassing entertainment, fitness, commerce, health, education, and so on. This "one place" portal would have to draw data from millions of downstream users. It may be more realistic to access sector specific data.

It may be more reasonable to obligate data fiduciaries to make available on demand, or at all times, on line, through the provision of a consent dashboard, a list of all data processors or fiduciaries it has received from or shared personal data with, the categories of data and the purpose.

18. (*1*) The data principal shall where necessary, having regard to the purposes for which personal data is being processed, subject to such conditions and in such manner as may be specified by regulations, have the right to-

(*a*) the correction of inaccurate or misleading personal data;

(*b*) the completion of incomplete personal data;

(*c*) the updating of personal data that is out-of-date; and

(*d*) the erasure of personal data which is no longer necessary for the purpose for which it was processed.

Consider adding (e) determine the fate of the data (transfered control or deletion) after the principal is deceased or incapacitated

In healthcare, (d) may need to be truncated to "the permissible erasure of personal data," as patients should have the right to withdraw their records or major components therein, from providers. We include the term "permissible," as there may be notifiable diseases that providers have a right to know to protect themselves from occupational hazards. The clause "for the purpose for which it was processed," may be problematic, as an electronic health record consists of data generated over time, most of which has fulfilled the purpose for which it was created, but may in the future play a role in informing future treatments or strategies. Health data specific regulations will need to define what medical history, if any, may not be deleted.

(*2*) Where the data fiduciary receives a request under sub-section (*1*), and the data fiduciary does not agree with such correction, completion, updation or erasure having regard to the purposes of processing, such data fiduciary shall provide the data principal with adequate justification in writing for rejecting the application**.**

(*3*) Where the data principal is not satisfied with the justification provided by the data fiduciary under sub-section (*2*), the data principal may require that the data fiduciary take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed by the data principal.

This could be rephrased for clarity. It seems to require that data that has been disputed by the patients, but not corrected by the fiduciary, would need an annotation that such data are disputed. To enforce this, the data fiduciaries will need to identify (or develop) interoperability standards that allow such information to be transmitted (and understood).

(*4*) Where the data fiduciary corrects, completes, updates or erases any personal data in accordance with sub-section (*1*), such data fiduciary shall also take necessary steps to notify all relevant entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion, updation or erasure, particularly where such action may have an impact on the rights and interests of the data principal or on decisions made regarding them.

Consider time limitations on both, the ability of principals (in this case, patients) to dispute data, and on the obligations of fiduciaries to change data that may have been transmitted a long time ago. While necessary, this obligation - without such time constraints - placed undue and unenforceable burden on data fiduciaries. Hospital A may have shared data with another hospital B, to which a patient may have been transferred, and Hospital B may have passed on the data to insurance companies for legitimate purposes. What if Hospital B is out of business, when the patient returns six years later, requesting that his record be modified? Hospital A will have no knowledge that the data was passed on to the insurance company.

Also, this clause is in direct conflict with the earlier sections requiring time and purpose limitation. Data that have been deleted after use, but after being passed on, are not available for rectification. A time stipulation is therefore of the essence. Medical records, for example, may be rectified within a year, for example.

19. (*1*) Where the processing has been carried out through automated means, the data principal shall have the right to—

(*a*) receive the following personal data in a structured, commonly used and machine-readable format—

(*i*) the personal data provided to the data fiduciary;

(*ii*) the data which has been generated in the course of provision of services or use of goods by the data fiduciary; or

(*iii*) the data which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained; and

In healthcare this provision has several useful applications. It lays the foundation for health data interoperability, and may require additional regulations that help enforce (and provide resources for such implementation. 19.1(iii) may refer to AI algorithms, and the clause requires that the output of the AI algorithm be made available to the principal. In

healthcare, additional regulations may be considered that minimize the blackbox nature of such algorithms, and that lay out the conditions under which such blackbox algorithms may be permissible.

In healthcare, it is important to maintain "immutability" of data. This is done in electronic health records, for example, by maintaining timestamps of all corrections. Such time/date stamps must be maintained by the fiduciary for all processing requests, including corrections to old data by either other fiduciaries, processors or principals. Such immutability plays a central role in preventing fraud.

(*b*) have the personal data referred to in clause (*a*) transferred to any other data fiduciary in the format referred to in that clause.

This is critical to health data portability, and cannot be over emphasized. Health data specific regulations should stipulate the relevant standards and formats.

(*2*) The provisions of sub-section (*1*) shall not apply where—

(*a*) processing is necessary for functions of the State or in compliance of law or order of a court under section 12;

This clause should be deleted. Its intention is not clear. In healthcare, it would absolve all state services from making their data interoperable, portable or available in a useable format.

(*b*) compliance with the request in sub-section (*1*) would reveal a trade secret of any data fiduciary or would not be technically feasible .

The "technical feasibility" clause will allow data fiduciaries to abrogate their responsibility to data principals. Sector-wise regulations may allow a transition time, to allow data fiduciaries to develop the technical capacity to do so, but to give the fiduciaries the option of claiming lack of technical feasibility is against the spirit of this law.

It is the expense associated with feasibility that may be prohibitive and may require additional provisions.

20. (*1*) The data principal shall have the right to restrict or prevent the continuing disclosure of his personal data by a data fiduciary where such disclosure —
(*a*) has served the purpose for which it was collected or is no longer necessary for the purpose;

(*b*) was made with the consent of the data principal under section 11 and such consent has since been withdrawn; or

(*c*) was made contrary to the provisions of this Act or any other law for the time being in force.

In healthcare, as data changes hands multiple times, over times, space and jurisdictions, it would be hard for principals to keep track of where their data are. This right to erasure may sometimes be in conflict with other obligations under the law to maintain the data for longer periods of time, and difficult to enforce.

Consider including "(d) is not willed by the data principal to the executors of her estate, or heirs, in the event of death.."

(*2*) The rights under sub-section (*1*) may be enforced only on an order of the Adjudicating Officer made on an application filed by the data principal, in such form and manner as may be prescribed, on any of the grounds specified under clauses (*a*), (*b*) or clause (*c*) of that sub-section:

This does not seem scalable in a cost-effective manner, and seems to be against the spirit of the law. It should not be cumbersome for data principals to request corrections or erasures; regulations may be considered to allow cost sharing so as to not put undue burden on either party.

Provided that no order shall be made under this sub-section unless it is shown by the data principal that his right or interest in preventing or restricting the continued disclosure of his personal data overrides the right to freedom of speech and expression and the right to information of any other citizen.

A second proviso be added under sub-clause 20.(2) as follows:
Restrictions may also be put on modifications or erasures, if the processing of certain data is necessary for population health purposes (in the public interest), for example for protecting against serious cross-border pandemics. For example, it may be reasonable for the MoHFW to request that a positive diagnosis of COVID-19 (novel coronavirus) may not be deleted from records, until the pandemic has abated, in the interest of contact tracing, surveillance and public health. Such exemptions cannot be made ad hoc and must be made through responsive regulatory channels.

(*3*) The Adjudicating Officer shall, while making an order under sub-section (*2*), having regard to—

(*a*) the sensitivity of the personal data;
(*b*) the scale of disclosure and the degree of accessibility sought to be restricted or prevented;
(*c*) the role of the data principal in public life;
(*d*) the relevance of the personal data to the public; and
(*e*) the nature of the disclosure and of the activities of the data fiduciary, particularly whether the data fiduciary systematically facilitates access to personal data and whether the activities shall be significantly impeded if disclosures of the relevant nature were to be restricted or prevented.

3(c) seems open to interpretation. Do data principals in public life have a greater obligation to be transparent, or a greater protection against the intrusion of their privacy? If a person running for public office (or in public office) requests the deletion of certain medical diagnoses, does the adjudicating officer have a right to deny this request? Such differential treatment is problematic, and is one more reason why the provision of an adjudicating officer is not a feasible option. An automated (or decentralized) process would not require the identity of the person to be known, and could adjudicate on the merit of the request for erasure or modification. Please refer to earlier comments on role-based address. The principal's identity should be decoupled from information about the nature of data and purpose for alteration that are presented to the adjudicator whatever her / its form.

(*4*) Where any person finds that personal data, the disclosure of which has been restricted or prevented by an order of the Adjudicating Officer under sub-section (*2*), does not satisfy the conditions referred to in that sub-section, he may apply for the review of that order to the Adjudicating Officer in such manner as may be prescribed, and the Adjudicating Officer shall review his order.

(*5*) Any person aggrieved by an order made under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal.

21. (*1*) The data principal, for exercising any right under this Chapter, except the right under section 20, shall make a request in writing to the data fiduciary either directly or through a consent manager with the necessary information as regard to his identity, and the data fiduciary shall acknowledge the receipt of such request within such period as may be specified by regulations.

Consider revising sub-clause 21(1) as follows:

For exercising any right under this Chapter, except the right under section 20, the data principal or surrogate, including parent or guardian, as may be prescribed by regulations, shall make a request or grant access in writing, online or offline, to the data fiduciary either directly or through a consent manager with the necessary information as regard to his identity, and the data fiduciary shall acknowledge the receipt of such request within such period as may be specified by regulations.

We have included “grant request” through a consent manager, to facilitate asynchronous transfer of health data across service providers once consent is made. Consent can always be withdrawn but need not be sought for each transaction, except where required by law.

(*2*) For complying with the request made under sub-section (*1*), the data fiduciary may charge such fee as may be specified by regulations:

Provided that no fee shall be required for any request in respect of rights referred to in clause (*a*) or (*b*) of sub-section (*1*) of section 17 or section 18.

(*3*) The data fiduciary shall comply with the request under this Chapter and communicate the same to the data principal, within such period as may be specified by regulations.

(*4*) Where any request made under this Chapter is refused by the data fiduciary, it shall provide the data principal the reasons in writing for such refusal and shall inform the data principal regarding the right to file a complaint with the Authority against the refusal, within such period and in such manner as may be specified by regulations.

(*5*) The data fiduciary is not obliged to comply with any request under this Chapter where such compliance shall harm the rights of any other data principal under this Act.

CHAPTER VI

TRANSPARENCY AND ACCOUNTABILITY MEASURES

22. (*1*) Every data fiduciary shall prepare a privacy by design policy, containing—

The quality and legibility of the policy is a deterrent to consent or being informed, which sort of obliviates the purpose of the law in the eyes of the consumer. We recommend that the government publish model policies, perhaps by sector, where necessary. In healthcare, for example, there de-identification should begin as close to source as possible. There is no reason why administrators should have access to identifiable information or details about patient's medical histories that are not relevant to their functioning.

(*a*) the managerial, organisational, business practices and technical systems designed to anticipate, identify and avoid harm to the data principal;
(*b*) the obligations of data fiduciaries;
(*c*) the technology used in the processing of personal data is in accordance with commercially accepted or certified standards;

The terms "commercially accepted or certified standards" is not specific enough. Consider deleting "commercially accepted" and list 'certified standards.' To scale, the DPA may consider allowing third-party certification.

(*d*) the legitimate interests of businesses including any innovation is achieved without compromising privacy interests;

Consider rephrasing as below: The legitimate business interests of the data fiduciary, including research and development for innovation, is achieved without compromising privacy interests;

(*e*) the protection of privacy throughout processing from the point of collection to deletion of personal data;
(*f*) the processing of personal data in a transparent manner; and
(*g*) the interest of the data principal is accounted for at every stage of processing of personal data.

(*2*) Subject to the regulations made by the Authority, the data fiduciary may submit its privacy by design policy prepared under sub-section (*1*) to the Authority for certification within such period and in such manner as may be specified by regulations.

Consider offering a selection of model policies - if the key differences between policies are widely known, data principals will be able to make meaningful choices. Consider, for example, categories of Creative Common Licenses. Users can immediately recognize (or look up) what is permitted and what isn't under the CC. If every fiduciary is allowed to develop a unique policy, users will continue to face the challenges they face today - of coerced, uninformed consent obtained by inundating the consumer with long pages of legalese. In healthcare, this "consent" is typically obtained at hospital registration or enrollment, or by the bedside - circumstances that can hardly be considered non-coercive.

(3) The Authority, or an officer authorised by it, shall certify the privacy by design policy on being satisfied that it complies with the requirements of sub-section (1).

As per our recommendation below, if a menu of polices (or options) are published by the DPA, this certification process will become sustainable and scale-able (and probably may not be required). However, certification of millions of policies seems unenforceable.

(*4*) The privacy by design policy certified under sub-section (*3*) shall be published on the website of the data fiduciary and the Authority.

For consent to be meaningful, this policy should be more readily accessible, and not merely "on the website." Healthcare services will increasingly be accessed through apps, and easily understandable data sharing choices should be available through the apps, as they are now, for most apps, since the GDPR in Europe, and the state of California's new Data Policy Law. A survey of existing choices available to consumers under this regime shows that here's a wide continuum available through apps. The choices depend on what a company considers to be legitimate business interest and the consent flows implemented often represent the risk tolerance of the authors of the app, whenever there is ambiguity in the law. Unfortunately, "legitimate business interest" is designed to be ambiguous.

Some healthcare services, like chemists or labs, may not be accessed online, and these brick and mortar establishments should be expected to declare their policies at prominent, accessible locations in their establishment, similar to the Patient's Bill of Rights posted in waiting rooms in US hospitals or handed over along with paper documents, including at several hospitals in India.

23. (*1*) Every data fiduciary shall take necessary steps to maintain transparency in processing personal data and shall make the following information available [s1] in such form and manner as may be specified by regulations—

(a) the categories of personal data generally collected and the manner of such collection;
(b) **the purposes for which personal data is generally processed;**

In healthcare, it will be important to stipulate what level of detail is expected from the data fiduciary. Will it suffice to say, for example, that "your data may be used for clinical research and quality improvement," or will the fiduciary be expected to provide a dashboard with updates about every trial or database the data have been shared with, as is required by earlier sections of this Bill?

(c) any categories of personal data processed in exceptional situations or any exceptional purposes of processing that create a risk of significant harm;
(d) the existence of and the procedure for exercise of rights of data principal under Chapter V and any related contact details for the same;
(e) the right of data principal to file complaint against the data fiduciary to the Authority;
(f) where applicable, any rating in the form of a data trust score that may be accorded to the data fiduciary under sub-section (*5*) of section 29;
(*g*) where applicable, information regarding cross-border transfers of personal data that the data fiduciary generally carries out; and
(h) any other information as may be specified by regulations.

(*2*) The data fiduciary shall notify, from time to time, the important operations in the processing of personal data related to the data principal in such manner as may be specified by regulations.

This section needs to be more specific: notify whom and how, to what purpose? How will the costs of such notification be borne by smaller enterprises? Frequency should be specified. In healthcare, for example, the account aggregatory may be required to post each time the principal's health data is posted. This notification may be available on a consent dashboard, or pushed via a notification to the mobile device, depending on what technology, regulations and costs, allow.

(*3*) The data principal may give or withdraw his consent to the data fiduciary through a consent manager .

In healthcare, this provision is a central component of the architecture proposed by academic experts, NITI Aayog's Strategy and Approach Document for the National Health Stack and the Ministry of Health and Family Welfare's National Digital Health Blueprint.

Sector specific regulations will be required to make such provisions meaningfully accessible to those with limited access or ability to navigate online platforms. We recommend that this phrase be revised to:

The data fiduciary will allow data principals to give or withdraw consent in such as manner as to make such choice meaningful, accessible and non-discriminatory to those with limited access to or ability to navigate digital platforms.

(*4*) Where the data principal gives or withdraws consent to the data fiduciary through a consent manager, such consent or its withdrawal shall be deemed to have been communicated directly by the data principal.

Consider including "or surrogate" in this clause.

(*5*) The consent manager under sub-section (*3*), shall be registered with the Authority in such manner and subject to such technical, operational, financial and other conditions as may be specified by regulations.

***Explanation.*—For the purposes of this section, a "consent manager" is a data fiduciary which enables a data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platform .**

Require meaningful alternatives for the millions in India that do not have access to or the ability to navigate digital platforms, with consideration to costs associated with such alternatives, and the possible discrimination that may arise when such alternatives are not available.

Consider, for example, an opt-out consent option offered at a hospital (data fiduciary), where patients need to access a digital platform to prevent their data being shared with third-parties. Such an option would in effect be meaningless to many who do not have such access. Therefore, where such options are not feasible, regulation should favor the data principal - the onus of the additional effort made to gain consent from these data principals should be on the data fiduciary and not the other way around.

24. (*1*) Every data fiduciary and the data processor shall, having regard to the nature, scope and purpose of processing personal data, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, implement necessary security safeguards, including—

(*a*) use of methods such as de-identification and encryption;

(*b*) steps necessary to protect the integrity of personal data; and

(*c*) steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.

Consider rephrasing:
Every data fiduciary and the data processor shall, having regard to the nature, scope and purpose of processing personal data, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, implement necessary security safeguards, to ensure privacy by design, including—

(*a*) use of methods such as de-identification, aggregation, encryption, anonymization and other evolving technologies to protect privacy;

Data fiduciaries must be required to address the advances in machine learning and AI that increasingly make possible the re-identification of what was assumed to be de-identified or anonymized data. Consider adding a sub-clause (d):

"(d) review of and updating of its architecture to respond to advances in digital technology"

(*2*) Every data fiduciary and data processor shall undertake a review of its security safeguards periodically in such manner as may be specified by regulations and take appropriate measures accordingly.

25. ***(1)*** **Every data fiduciary shall by notice inform the Authority about the breach of any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal.**

(2) The notice referred to in sub-section (1) shall include the following particulars, namely:—

(a) nature of personal data which is the subject-matter of the breach;
(b) number of data principals affected by the breach;
(c) possible consequences of the breach; and
(d) action being taken by the data fiduciary to remedy the breach.

Modify sub-clause 25.(2)(d) as follows:
Action being taken by the data fiduciary to remedy the breach and to prevent such breaches in the future.

(3) The notice referred to in sub-section (1) shall be made by the data fiduciary to the Authority as soon as possible and within such period as may be specified by regulations, following the breach after accounting for any period that may be required to adopt any urgent measures to remedy the breach or mitigate any immediate harm.

(4) Where it is not possible to provide all the information specified in sub-section (2) at the same time, the data fiduciary shall provide such information to the Authority in phases without undue delay.

Consider stipulating time frames here, either through this Bill, or via subsequent regulations.

(*5*) Upon receipt of a notice, the Authority shall determine whether such breach should be reported by the data fiduciary to the data principal, taking into account the severity of the harm that may be caused to such data principal or whether some action is required on the part of the data principal to mitigate such harm.

All data breaches should be reported, and the communication should include the severity of harm that was caused or may be caused. The notification should include instructions for steps that the data principal needs to take (if any) to secure their data (for example, change passwords, or monitor their credit score); and post the remedial measures that have since been implemented by the data fiduciary.

(*6*) The Authority may, in addition to requiring the data fiduciary to report the personal data breach to the data principal under sub-section (*5*), direct the data fiduciary to take appropriate remedial action as soon as possible and to conspicuously post the details of the personal data breach on its website.

Not all data fiduciaries may have a website.

(*7*) The Authority may, in addition, also post the details of the personal data breach on its website.

Modify sub-clause 25.(7) as follows:
The Authority *shall*, in addition, also post the details of the personal data breach on its website. Requiring the DPA to do this supports the spirit of this law and makes such information more meaningfully accessible to data principals.

For example, in the United States, the USDA maintains a running list of all food recalls. That allows consumers to visit a single site to see whether the food they own is subject to a recall. It is an undue burden for a consumer to go to the website of each individual food manufacturer. Therefore we recommend that the Authority always post the details of every reported personal data breach.

Clarification requested: what language will all the notifications mentioned in the Bill be mandated or available in? We recommend that notifications be made in English, in the state language, and if the data principal has expressed a preference in a language of her choice.

26 (*1*) The Authority shall, having regard to the following factors, notify any data fiduciary or class of data fiduciary as significant data fiduciary, namely:—

(*a*) volume of personal data processed;

(*b*) sensitivity of personal data processed;

(*c*) turnover of the data fiduciary;

(*d*) risk of harm by processing by the data fiduciary;

(*e*) use of new technologies for processing; and

(*f*) any other factor causing harm from such processing.

Note: it is likely that most data fiduciaries handling health data may therefore be considered significant health data fiduciaries, including several agencies in both the central and state governments, and who should be subject to the same regulations.

(*2*) The data fiduciary or class of data fiduciary referred to in sub-section (*1*) shall register itself with the Authority in such manner as may be specified by regulations.

(*3*) Notwithstanding anything in this Act, if the Authority is of the opinion that any processing by any data fiduciary or class of data fiduciary carries a risk of significant harm to any data principal, it may, by notification, apply all or any of the obligations specified in sections 27 to 30 to such data fiduciary or class of data fiduciary as if it is a significant data fiduciary.

(4) Notwithstanding anything contained in this section, any social media intermediary,-
(*i*) with users above such threshold as may be notified by the Central Government, in consultation with the Authority; and
(*ii*) whose actions have, or are likely to have a significant impact on electoral democracy, security of the State, public order or the sovereignty and integrity of India,

shall be notified by the Central Government, in consultation with the Authority, as a significant data fiduciary:

Provided that different thresholds may be notified for different classes of social media intermediaries.

Explanation.—For the purposes of this sub-section, a "social media intermediary" is an intermediary who primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services, but shall not include intermediaries which primarily,—

(*a*) enable commercial or business oriented transactions;
(*b*) provide access to the Internet;

(*c*) in the nature of search-engines, on-line encyclopedias, e-mail services or on-line storage services

27. (*1*) Where the significant data fiduciary intends to undertake any processing involving new technologies or large scale profiling or use of sensitive personal data such as genetic data or biometric data, or any other processing which carries a risk of significant harm to data principals, such processing shall not be commenced unless the data fiduciary has undertaken a data protection impact assessment in accordance with the provisions of this section.

(2) The Authority may, by regulations specify, such circumstances, or class of data fiduciary, or processing operation where such data protection impact assessment shall be mandatory, and also specify the instances where a data auditor under this Act shall be engaged by the data fiduciary to undertake a data protection impact assessment.

(3) A data protection impact assessment shall, inter alia, contain —

(a) detailed description of the proposed processing operation, the purpose of processing and the nature of personal data being processed;
(b) assessment of the potential harm that may be caused to the data principals whose personal data is proposed to be processed; and
(c) measures for managing, minimising, mitigating or removing such risk of harm.

(4) Upon completion of the data protection impact assessment, the data protection officer appointed under sub-section (1) of section 30, shall review the assessment and submit the assessment with his finding to the Authority in such manner as may be specified by regulations.

(5) On receipt of the assessment and its review, if the Authority has reason to believe that the processing is likely to cause harm to the data principals, the Authority may direct the data fiduciary to cease such processing or direct that such processing shall be subject to such conditions as the Authority may deem fit.

28. (1) The significant data fiduciary shall maintain accurate and up-to-date records of the following, in such form and manner as may be specified by regulations, namely:—
(a) important operations in the data life-cycle including collection, transfers, and erasure of personal data to demonstrate compliance as required under section 10;
(b) periodic review of security safeguards under section 24;
(c) data protection impact assessments under section 27; and
(d) any other aspect of processing as may be specified by regulations.

(2) Notwithstanding anything contained in this Act, this section shall also apply to the State.

(3) Every social media intermediary which is notified as a significant data fiduciary under sub-section (4) of section 26 shall enable the users who register their service from India, or use their services in India, to voluntarily verify their accounts in such manner as may be prescribed.

(4) Any user who voluntarily verifies his account shall be provided with such demonstrable and visible mark of verification, which shall be visible to all users of the service, in such manner as may be prescribed.

29. (*1*) The significant data fiduciary shall have its policies and the conduct of its processing of personal data audited annually by an independent data auditor under this Act.

As noted earlier, by the definition provided, hundreds if not thousands of health data fiduciaries are likely to be notified as "significant." How will this auditing process scale? It is not likely to be implementable or enforceable.

(*2*) The data auditor shall evaluate the compliance of the data fiduciary with the provisions of this Act, including—

(*a*) clarity and effectiveness of notices under section 7;
(*b*) effectiveness of measures adopted under section 22;
(*c*) transparency in relation to processing activities under section 23
(*d*) security safeguards adopted pursuant to section 24;
(*e*) instances of personal data breach and response of the data fiduciary, including the promptness of notice to the Authority under section 25;
(*f*) timely implementation of processes and effective adherence to obligations under sub-section (*3*) of section 28; and
(*g*) any other matter as may be specified by regulations.

Revise 29(2) to:
The data auditor shall evaluate the compliance of the *significant* data fiduciary with the provisions of this Act, including—

(*3*) The Authority shall specify, by regulations, the form and procedure for conducting audits under this section.

(*4*) The Authority shall register in such manner, the persons with expertise in the area of information technology, computer systems, data science, data protection or privacy, possessing such qualifications, experience and eligibility having regard to factors such as independence, integrity and ability, as it may be specified by regulations, as data auditors under this Act.

Recommend adding the phrase “information governance.” to the list of areas in which persons may have expertise.

(*5*) A data auditor may assign a rating in the form of a data trust score to the data fiduciary pursuant to a data audit conducted under this section.

(*6*) The Authority shall, by regulations, specify the criteria for assigning a rating in the form of a data trust score having regard to the factors mentioned in sub-section (*2*).

(*7*) Notwithstanding anything contained in sub-section (*1*), where the Authority is of the view that the data fiduciary is processing personal data in such manner that is likely to cause harm to a data principal, the Authority may direct the data fiduciary to conduct an audit and shall appoint a data auditor for that purpose.

30. (*1*) Every significant data fiduciary shall appoint a data protection officer possessing such qualification and experience as may be specified by regulations for carrying out the following functions—

(*a*) providing information and advice to the data fiduciary on matters relating to fulfilling its obligations under this Act;

(*b*) monitoring personal data processing activities of the data fiduciary to ensure that such processing does not violate the provisions of this Act;

(*c*) providing advice to the data fiduciary on carrying out the data protection impact assessments, and carry out its review under sub-section (*4*) of section 27;

(*d*) providing advice to the data fiduciary on the development of internal mechanisms to satisfy the principles specified under section 22;

(*e*) providing assistance to and co-operating with the Authority on matters of compliance of the data fiduciary with the provisions under this Act;

(*f*) act as the point of contact for the data principal for the purpose of grievances redressal under section 32; and

(*g*) maintaining an inventory of records to be maintained by the data fiduciary under section 28.

(*2*) Nothing contained in sub-section (*1*) shall prevent the data fiduciary from assigning any other function to the data protection officer, which it may consider necessary.

It must also be ensured that the Data Protection Officer does not have a conflict of interest that may prevent her from fulfilling her duties responsibly. A similar obligation is placed under the GDPR. The European Data Protection Supervisor recommends that conflicts of interests may be avoided by ensuring that the DPO is not the same as the data fiduciary (such as if she was the head of human resources), that she is not an employee on a short-term or fixed contract, she does not report to a direct superior and she is responsible for managing her own budget.

(*3*) The data protection officer appointed under sub-section (*1*) shall be based in India and shall represent the data fiduciary under this Act.

31. (*1*) The data fiduciary shall not engage, appoint, use or involve a data processor to process personal data on its behalf without a contract entered into by the data fiduciary and such data processor.

(*2*) The data processor referred to in sub-section (*1*) shall not engage, appoint, use, or involve another data processor in the processing on its behalf, except with the authorisation of the data fiduciary and unless permitted in the contract referred to in sub-section (*1*).

(3) The data processor, and any employee of the data fiduciary or the data processor, shall only process personal data in accordance with the instructions of the data fiduciary and treat it confidential.

We recommend that sub-clause 31.(3) be modified as follows to correct a grammatical error:

"The data processor, and any employee of the data fiduciary or the data processor, shall only process personal data in accordance with the instructions of the data fiduciary and treat it as confidential."

CHAPTER VIII

EXEMPTIONS

35. Where the Central Government is satisfied that it is necessary or expedient,—

(i) in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order; or

(ii) for preventing incitement to the commission of any cognizable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, it may, by order, for reasons to be recorded in writing, direct that all or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data, as may be specified in the order subject to such procedure, safeguards and oversight mechanism to be followed by the agency, as may be prescribed.

We note that this provision is over-broad and may be violative of the three-pronged requirement for a reasonable restriction on the right to privacy laid down by the Supreme Court in Puttaswamy v Union of India. Such a restriction is only permissible if there is a specific law permitting it, there is a legitimate state aim and the restriction place is proportional to the aim sought to be achieved.

Explanation.—For the purposes of this section,—
(i) the term "cognizable offence" means the offence as defined in clause (c) of section 2 of the Code of Criminal Procedure, 1973;

(*ii*) the expression "processing of such personal data" includes sharing by or sharing with such agency of the Government by any data fiduciary , data processor or data principal.

36. The provisions of Chapter II except section 4, Chapters III to V, Chapter VI except section 24, and Chapter VII shall not apply where—

(*a*) personal data is processed in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of any law for the time being in force;
(*b*) disclosure of personal data is necessary for enforcing any legal right or claim, seeking any relief, defending any charge, opposing any claim, or obtaining any legal advice from an advocate in any impending legal proceeding;
(*c*) processing of personal data by any court or tribunal in India is necessary for the exercise of any judicial function;

(*d*) personal data is processed by a natural person for any personal or domestic purpose, except where such processing involves disclosure to the public, or is undertaken in connection with any professional or commercial activity; or
(*e*) processing of personal data is necessary for or relevant to a journalistic purpose, by any person and is in compliance with any code of ethics issued by the Press Council of India, or by any media self-regulatory organisation.

37. The Central Government may, by notification, exempt from the application of this Act, the processing of personal data of data principals not within the territory of India, pursuant to any contract entered into with any person outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law.

38. Where the processing of personal data is necessary for research, archiving, or statistical purposes, and the Authority is satisfied that—

(*a*) the compliance with the provisions of this Act shall disproportionately divert resources from such purpose;

The term 'disproportionately' is too vague and this provision is prone to being abused. Instead of a disproportionate diversion of resources, we recommend that a risk-based categorisation be adopted. It is not the weight of resources, but the risks to data principals and their privacy that should constitute the criteria for waiver. Data protection will always require resources.

We recommend the deletion of this sub-clause, or rephrasing it to reflect such risk stratification: (a) non-compliance with the provisions of this Act shall pose no to minimal risks to data principals, and any such processing will only be undertaken as permitted under sector-specific regulations.

(In the case of healthcare, for example, research that involves very-low risk to participants (as determined by an Ethics Committee under the Drugs and Cosmetics Act, 1940), may be exempt from complying with the requirements under this Act).

(b) the purposes of processing cannot be achieved if the personal data is anonymised;

(c) the data fiduciary has carried out de-identification in accordance with the code of practice specified under section 50 and the purpose of processing can be achieved if the personal data is in de-identified form;

(*d*) the personal data shall not be used to take any decision specific to or action directed to the data principal; and

Medical research, whether traditional or with modern tools, including with artificial intelligence and machine learning models, may sometimes have direct relevance to the health and lives of the data principals studied. We therefore recommend that this sub-clause be limited to decisions that cause harm or are discriminatory.

The sub-clause should be re-drafted as follows:

"(*d*) the personal data shall not be used to take any decision specific to or action directed at the data principal which discriminates against or causes harm to the data principal; and"

(e) the personal data shall not be processed in the manner that gives rise to a risk of significant harm to the data principal,

it may, by notification, exempt such class of research, archiving, or statistical purposes from the application of any of the provisions of this Act as may be specified by regulations.

39. (*1*) The provisions of sections 7, 8, 9, clause (*c*) of sub-section (*1*) of section 17 and sections 19 to 32 shall not apply where the processing of personal data by a small entity is not automated.

(*2*) For the purposes of sub-section (*1*), a "small entity" means such data fiduciary as may be classified, by regulations, by Authority, having regard to—

(*a*) the turnover of data fiduciary in the preceding financial year;

(*b*) the purpose of collection of personal data for disclosure to any other individuals or entities; and

(*c*) the volume of personal data processed by such data fiduciary in any one day in the preceding twelve calendar months.

40. (*1*) The Authority shall, for the purposes of encouraging innovation in artificial intelligence, machine-learning or any other emerging technology in public interest, create a Sandbox .

The purpose of regulatory sandboxes is to enable innovation by relaxing existing regulations for a defined time period, and possibly in a specific jurisdiction. For example, if the existing law mandates that community health workers pay a visit to patients with disease X once every week, and an AI algorithm claims that it may be able to identify patients at a higher risk of non-compliance, a regulatory sandbox would allow the relevant state agency to evaluate the AI algorithm in a certain district for a set period of time before rejecting it or rolling it out en masse. At no point, should the data principals not enjoy the protection of the law.

The “sandbox” should allow entities to apply for exceptions to specific regulations under this or another law, but under no circumstances should it provide a blanket exemption.

(2) Any data fiduciary whose privacy by design policy is certified by the Authority under sub-section (3) of section 22 shall be eligible to apply, in such manner as may be specified by regulations, for inclusion in the Sandbox created under sub-section (1).
(3) Any data fiduciary applying for inclusion in the Sandbox under sub-section (2) shall furnish the following information, namely:—
(a) the term for which it seeks to utilise the benefits of Sandbox, provided that such term shall not exceed twelve months;
(b) the innovative use of technology and its beneficial uses;
(c) the data principals or categories of data principals participating under the proposed processing; and
(d) any other information as may be specified by regulations.

(*4*) The Authority shall, while including any data fiduciary in the Sandbox, specify—
(*a*) the term of the inclusion in the Sandbox, which may be renewed not more than twice, subject to a total period of thirty-six months;

Permit recourse for extension under exceptional circumstances, such as a new public health AI tool for a devastating but infrequently occurring event like an epidemic or pandemic.

(*b*) the safeguards including terms and conditions in view of the obligations under clause (*c*) including the requirement of consent of data principals participating under any licensed activity, compensation to such data principals and penalties in relation to such safeguards; and
(*d*) that the following obligations shall not apply or apply with modified form to such data fiduciary, namely:—
(i) the obligation to specify clear and specific purposes under sections 4 and 5;
(ii) limitation on collection of personal data under section 6; and
(iii) any other obligation to the extent, it is directly depending on the obligations under sections 5 and 6; and
(iv) the restriction on retention of personal data under section 9.

CHAPTER IX

DATA PROTECTION AUTHORITY OF INDIA

41. (*1*) The Central Government shall, by notification, establish, for the purposes of this Act, an Authority to be called the Data Protection Authority of India.
(*2*) The Authority referred to in sub-section (*1*) shall be a body corporate by the name aforesaid, having perpetual succession and a common seal, with power, subject to the provisions of this Act, to acquire, hold and dispose of property, both movable and immovable,
and to contract and shall, by the said name, sue or be sued.

(*3*) The head office of the Authority shall be at such place as may be prescribed.

(*4*) The Authority may, with the prior approval of the Central Government, establish its offices at other places in India.

It is unclear the extent to which the jurisdiction of the Data Protection Authority will extend to entities operating outside India.

For instance, if a company based in the US develops an app that goes on the Google Play Store and that collects data for storage outside of India, how is the DPA going to know about that? Will Google be required to include in the Google Play Store tools for specifying a registered Data Protection Officer (DPO) in India? Or is it the responsibility of the app developer to inform the government of the registered DPO? Is there any mechanism for verifying that the registered DPO actually exists? What happens to the company's app if it is found to be in violation of the Data Protection Law? Does the DPA have a mechanism to force Google to remove it from the Google Play Store? How will the DPA collect fines levied against the company? Through Google? Will the DPA have the authority to prevent the Google Play Store from allowing the company to continue to distribute my app?

We recommend that regulations specifically prescribe how the duties and obligations under this Act will apply to and be enforced against entities incorporated and primarily operating outside India - as the vast majority of healthcare apps and wearables currently tend to be.

42. (*1*) The Authority shall consist of a Chairperson and not more than six whole-time Members, of which one shall be a person having qualification and experience in law.

Given the very high stakes associated with health data exchange and its potential impact on the lives of hundreds of millions of Indias, on population health, and on medical science, we recommend that one person have background in medicine and health data science.

(*2*) The Chairperson and the Members of the Authority shall be appointed by the Central Government on the recommendation made by a selection committee consisting of—

(*a*) the Cabinet Secretary, who shall be Chairperson of the selection committee;
(*b*) the Secretary to the Government of India in the Ministry or Department dealing with the Legal Affairs; and

(*c*) the Secretary to the Government of India in the Ministry or Department dealing with the Electronics and Information Technology.

(*3*) The procedure to be followed by the Selection Committee for recommending the names under sub-section (*2*) shall be such as may be prescribed.

(*4*) The Chairperson and the Members of the Authority shall be persons of ability, integrity and standing, and shall have qualification and specialised knowledge and experience of, and not less than ten years in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, public administration, national security or related subjects

Domain specific experts be included as Members of the Authority. The Bill may also provide for the constitution of sub-committees or for consultation with external domain experts during the rulemaking process.

We recommend that Clause 42.(4) be modified as follows:
The Chairperson and the Members of the Authority shall be persons of ability, integrity and standing, and shall have qualification and/or specialised knowledge, competencies, skills and experience of, and not less than ten years in legal and/or technical aspects of privacy, data protection laws and practices, information technology, health informatics, data management, data science, data security, cyber-security and internet laws, public administration, public health, national security, sector-specific data protection practices or related subjects.

(*5*) A vacancy caused to the office of the Chairperson or any other member of the Authority shall be filled up within a period of three months from the date on which such vacancy occurs.

ADDITIONAL CLAUSE-SPECIFIC COMMENTS

53 (*7*) The Inquiry Officer may keep in its custody any books, registers, documents, records and other data produced under sub-section (*5*) for six months and thereafter shall return the same to the person by whom or on whose behalf such books, registers, documents, record and data are produced, unless an approval to retain such books, registers, documents, record and data for an additional period not exceeding three months has been obtained from the Authority.

This is unacceptable in healthcare, and will need careful consideration of sector specific regulations. The confiscation of data can cause interruption of care, with detrimental impact on the health and wellbeing of data principals. Access to "books, registers, documents, records and other data" implies access to personal data or sensitive personal health data, and may be against the objectives of the Bill. Auditing health data will require additional safeguards and accountability mechanisms to be incorporated to prevent the misuse of these provisions by auditors.

82. (*1*) Any person who, knowingly or intentionally—

(*a*) re-identifies personal data which has been de-identified by a data fiduciary or a data processor, as the case may be; or

(*b*) re-identifies and processes such personal data as mentioned in clause (*a*), without the consent of such data fiduciary or data processor, then, such person shall be punishable with imprisonment for a term not exceeding three years or with a fine which may extend to two lakh rupees or both.

Re-identification may be inadvertent due to advances in big data analytics, or sometimes, simply due to a small sample size. For example, health data about a patient with a rare disease, may allow data fiduciaries how are familiar with the patient to recognize her association with the data. Similarly, there are some tribal populations in India that are numerically small. Personal Data released on individuals from such populations, with or without metadata, can result in individual identification. We therefore recommend that this clause be amended to: If data are inadvertently re-identified it is incumbent on the data fiduciary to notify the DPA that re-identification occured, and include steps that were taken to prevent harm to the data principal, and to re-mask identities, and steps taken to prevent such recurrence in the future. The DPA should have the power to adjudicate such matters and levy or waive fines, based on the intent to cause harm, the fiduciary's data protection preparedness, and the harm caused.

(*b*) the data principal whose personal data is in question has explicitly consented to such re-identification or processing as per the provisions of this Act.

In the medical context, it is often the surrogate or guardian that gives consent on behalf of the person undergoing medical treatment and agreeing to their personal data being collected. For instance, the Mental Healthcare Act, 2017 allows people to appoint their Nominated Representative to make decisions on their behalf in situations when they may not have the mental capacity to do so themselves. The exception carved out in this provision should also account for surrogates or guardians.

We recommend that the clause be amended as follows:

“the data principal whose personal data is in question, their legal guardian or nominated representative, has explicitly consented to such re-identification or processing as per the provisions of this Act.”

***91 (2) Explanation*.—For the purposes of this sub-section, the expression "non-personal data " means the data other than personal data.**

As indicated earlier, in the domain of health, data that we have assumed so far to be non-personal, can be increasingly used to profile individuals and their health. Such distinctions warrant further attention. Non-personal data may need their own governance framework, as they pose their own sets of risks on their own, or when combined with other non-personal data. Where a data principal seeks care (based on the GPS locations of cancer hospitals or STD clinics) may reveal a lot more personal or even sensitive personal information about a data principal, than anticipated. See EU guidelines on non-personal data: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_2750