To :

The Director ,
Lok Sabha Secretariat ,
Room No: 152,
Parliament House Annexe,
New Delhi.

Date : 25/2/2020

Dear Sir/ Madam,

On behalf of DHIndia Association (Digital Health India Association), we hereby submit the feedback and comments on the Personal Data Protection (PDP) bill after taking feedback from our community, which was then collated and curated by our Legal and Medical experts, spear headed by Dr G. S. Jaiya. We hope that this feedback will be fruitful and beneficial to optimizing and making the bill robust, taking into account the context for our country and the Indian Healthcare domain.

Please find attached the feedback document referred to.

Assuring you of our best efforts and wishes for the success of the bill.

Best Regards,

Pramod

Dr Pramod D. Jacob (MBBS, MS- Medical Informatics) ,
CEO- DHIndia Association

Comments on the PDP Bill (373 of 2019)

A. General comments:

1. Though overall an excellent bill, there are a number of ambiguities in the definitions and in the text of some of its key provisions. Drafting improvements have therefore been suggested to make it clearer and precise. Some of the definitions in the PDP Bill (373 of 2019) have been reworded, rearranged and/or elaborated.
2. Many new definitions are essential to reduce ambiguity and clarify scope.
3. Most of the specific comments made and drafting changes proposed pertain to the health and medical domains, as these modifications are considered to be essential sincethe health domain specific bill, namely, the draft Digital Information Security in Healthcare Act ("DISHA") will no longer be enacted in view of the all encompassing PDP bill; please see the PIB note of July 16, 2019 at https://pib.gov.in/Pressreleaseshare.aspx?PRID=1578929
   Which states as follows:

   "MoHFW had drafted a "Digital Information Security in Healthcare Act (DISHA Act)" with the objective to ensure data privacy, confidentiality, reliability and security of digital health data. This Ministry forwarded the draft legislation to Ministry of Electronics and Information Technology (MeitY) for seeking their inputs and guidance.

   In response, it was informed that MeitY is in process of enacting 'Data Protection Framework on Digital Information Privacy, Security & Confidentiality' Act, which would be applicable in all domains including health. This act would provide the framework for the Ministry to utilize the patient data in programmes in a secured manner.

   Therefore, the Ministry submitted the draft DISHA Act to MeitY to be subsumed in the upcoming 'Data Protection Framework on Digital Information Privacy, Security & Confidentiality' Act to avoid the duplicity of effort. The Minister of State (Health and Family Welfare), Sh Ashwini Kumar Choubey stated this in a written reply in the Rajya Sabha here today."

   The PDP Bill and DISHA take a very different approach to protecting health data, not only in terms of the position of the individual, but also in terms of the terms, their definitions, the fundamental concepts, and the uses of sensitive personal/health data envisaged under each. The current draft has taken hardly anything from DISHA onboard.

4. At a few places the drafting of the provisions of the bill need improved clarity or specificity; therefore, appropriate amendments have been proposed.
5. At a number of places the phrase '...as may be prescribed by regulations' has been suggested to indicate that greater clarity or detail is needed which can be provided in the detailed sectoral regulations in due course.

Specific Comments:

1. Revised definitions:

    a. Biometric data

    Comment: Revised reworded, rearranged and elaborated definition proposed for biometric data:

    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.*

    References:

    https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-is-risky.html

    https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html

    https://www.biometricupdate.com/201401/explainer-footprint-identification

    b. Genetic data

    Comment: Revised definition proposed for genetic data by adding the word 'DNA' but the last phrase about 'analysis of a biological sample' has been proposed to be deleted as it is obvious and, therefore, redundant:

    As per Clause 3(19) "genetic data" means personal data relating to the inherited or acquired genetic (DNA) characteristics of a natural person which give unique information about the behavioural characteristics, physiology or the health of that natural person;

Further comment:

"People often view genetic information about themselves as private. Each person's genome, or full complement of DNA, is unique, but the specific variants within an individual's genome may be widely shared with biological relatives or even across the entire human population. This mixed character of the genome—as a uniquely individual assemblage of widely shared common elements—imbues it with a dual private and public significance that confounds any discussion of policy addressing genetic privacy.

On one hand, DNA has been conceptualized as a unique identifier and a person's book of life, which provides insights into many aspects of the person's future, although perhaps not as much as many people might think. This conceptualization leads many people to want to control who has access to genetic information about them and drives calls for strong privacy protection or even personal genetic data ownership. *On the other hand, genetic data are not limited to one individual, with information about one person revealing information about the person's close and distant biological relatives.* Only by studying genetic information from many people can the significance of the individual's variants be discerned. The importance of understanding the causes of health and disease has led some to argue that people have some obligation to share data about themselves for low-risk research. This public nature and value of the genome makes it difficult to decide what level of control individuals should have and how to provide appropriate privacy protections."

https://academic.oup.com/jlb/article/6/1/1/5489401

Recommendation: In view of the above comment, the question of DNA as a unique identifier should be looked into and the need for a more elaborate guidance be considered in determining the scope of the privacy related rights for it.

Comment: There can be no data about the future state of health. In addition language has been improved.

c. Health data: Revised definition proposed

Clause 3(28) "personal data" means data based on facts, opinions or personal assessments about or relating to a natural person who is directly

or indirectly identifiable, having regard to any physical, physiological, genetic, mental, economic, cultural or social characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, including a name, an identification number, location data, an online identifier or to one or more factors or any combination of such features with any other information, and shall also include any inference drawn from such data for the purpose of profiling;

Comment

In the PDP bill, the definitions of biometric data and genetic data refer to data principal, whereas the definitions of health data and personal data refer to natural person. The first two definitions have been modified to replace data principal by natural person.

d. Clause 3(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;

Comments

1. In this section, all terms are defined except the following: sex life, sexual orientation, caste or tribe.
2. It is suggested that these three terms should also be defined. In particular, definition of caste or tribe should be linked to one or more existing legislation on SC/ST only or also to definitions of OBCs included at the state level. https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/99649/119024/F1418240846/IND99649.pdf

2. NEW DEFINITIONS NEEDED
   a. Definition of “trade secret” needed.

      This term appears only in clause 19(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; (b) compliance with the request in sub-section (1) would reveal a trade secret of any data fiduciary or would not be technically feasible.

      Comment:

      It is necessary to find a balance between data protection rights and trade secret rights. A trade secret holder should be free not to disclose the output of their data processing (behavior evaluation, forecast, studies on life expectancy, personalized marketing plan, pricing, etc.) if disclosure can adversely affect their interests. In the absence of a national law on trade secrets in India it would be useful to define trade secrets in the PDP bill.

      <u>New definition of “trade secret” proposed as follows:</u>

      A **trade secret** refer to information:

      - which is not generally known or readily accessible, either in its entirety or in the precise arrangement and composition of its components, to the persons in the circles who normally deal with this type of information and is therefore of economic value,
      - which is subject to appropriate confidentiality measures by its lawful holder which are considered reasonable under the circumstances; and
      - in whose confidentiality the holder has a legitimate interest.

        https://helda.helsinki.fi/handle/10138/231948

   b. Definition of “data privacy” needed for the following reason:

      The Distinction: Data Privacy versus Protection

      In a nutshell, data protection is about securing data against unauthorized access. Data privacy is about authorized access — who has it and who

defines it. Another way to look at it is this: data protection is essentially a technical issue, whereas data privacy is a legal one.

These distinctions matter because they're woven deeply into the overarching issues of privacy and cybersecurity, both of which loom large in businesses, politics and culture. For industries subject to compliance standards, there are crucial legal implications associated with privacy laws. And ensuring data protection may not adhere to every required compliance standard.

According to the Storage Networking Industry Association (SNIA), the laws and regulations that cover "the management of personal information" are typically grouped under "privacy policy" in the United States and under "protection policy" in the EU and elsewhere.

The European Union's General Data Protection Regulation (GDPR), a supervisory authority that will go into effect May 25, 2018, requires businesses to protect the "personal data and privacy of EU citizens for transactions that occur within the EU." However, the GDPR's data protection law has a much different view of personal identification information than the US. GDPR compliance requires that companies use the same level of data protection for cookies as they do for stored personally identifiable information, such as social security numbers.

Data Privacy and Security: One Doesn't Ensure the Other

What's important to understand when comparing data privacy vs. data protection is that you can't ensure data privacy unless the personal data is protected by technology. If someone can steal personal data, its privacy is not guaranteed, which puts you at risk for identity theft and other personal security breaches. *But the opposite relationship isn't always true: personal data can be protected while still not being reliably private*.

How? When you swipe your credit card for a service provider, you're doing two things. First of all, you're trusting the service provider and payment system with your personal data protection — to make sure, among other things, shady cybercriminals and other third parties can't access your credit information without your consent. But you're also trusting them to honor your data privacy by not misusing the information even though you provided it to them.

The point is technology alone cannot ensure the privacy of personal data. Most privacy protection protocols are still vulnerable to authorized individuals who might access the data. The burden on these authorized individuals is, above all, about privacy law, not technology.

https://blog.ipswitch.com/data-privacy-vs-data-protection

Though most people agree on the importance of data privacy, and everyone agrees that data protection is at the heart of ensuring privacy, the definition of “data privacy” itself is notoriously complex.

None of the laws we mention in this article – the GDPR, the CCPA, or the HIPAA – define precisely what they mean by data privacy. Instead, the provisions they contain suggest a number of best practices, and spell out the rights of consumers and businesses. Since every piece of legislation is different, trying to define exactly what is meant by “privacy” can be extremely difficult.

https://www.varonis.com/blog/data-privacy/

Data privacy is about keeping your information from being sold or shared, while data protection focuses on keeping that information from hackers.The distinction between privacy and protection boils down to who we intend to share your data with versus how we plan to protect your data from everyone else. At the data access level, they mean the same thing. But in reality, protecting data from unauthorized access requires going beyond a simple ACL scheme and defending against all the vulnerabilities of the underlying systems.

https://www.forbes.com/sites/forbestechcouncil/2018/12/19/data-privacy-vs-data-protection-understanding-the-distinction-in-defending-your-data/#173bd54c50c9

New definition of “data privacy” proposed as follows:

Data privacy means ‘what data fiduciary or data processor who have collected your data lawfully can and should do with it and what rights or control the data principal has over that retention and use of personal data’.

https://blog.signaturit.com/en/gdpr-explicit-consent-from-your-clients#1

c. Definition of “innovation” needed; it also needs to be distinguished from research/research & development.

The word ‘innovation’ appears in sub-clauses 22(1)(d), 40(1), and 49(2)(k).

Sub-clause 49(2)(k) is about ‘promoting measures and undertaking research for innovation in the field of protection of personal data;’

Comment:

The words *innovation* and *invention* overlap semantically but are really quite distinct. Invention can refer to a type of musical composition, a falsehood, a discovery, or any product of the imagination. The sense of invention most likely to be confused with innovation is “a device, contrivance, or process originated after study and experiment,” usually something which has not previously been in existence. Innovation, for its part, can refer to something new or to a change made to an existing product,idea, or field. One might say that the first telephone was an invention, the first cellular telephone either an invention or an innovation, and the first smartphone an innovation.

New definition of “innovation” proposed as follows:

Innovation is the creation, development and implementation of a new product, process or service, with the aim of improving efficiency, effectiveness or competitive advantage.

https://drkenhudson.com/best-way-define-innovation/

d. Definition of “research” needed; it would be preferable to use the term ‘research and development’ (R&D)

The word ‘research’ appears in clauses 38, 49(2)(k), 50(6)(r)

The term research and development (R&D) is widely linked to innovation both in the corporate and government world or the public and private sectors. R&D allows a company to stay ahead of its competition. Without an R&D program, a company may not survive on its own and may have to rely on other ways to innovate such as engaging in mergers and acquisitions (M&A) or partnerships. Through R&D, companies can design new products and improve their existing offerings. R&D is separate from

most operational activities performed by a corporation. The research and/or development is typically not performed with the expectation of immediate profit. Instead, it is expected to contribute to the long-term profitability of a company.

New definition of “Research and Development” proposed:

Research and development (R&D, R+D, or R'n'D), also known as **research and technological development** (RTD), refers to innovative activities undertaken by a natural or legal person (such as a business, company or government entity) in developing new services or products, or improving existing services or products. Research and development constitutes the first stage of development of a potential new service or production process.

An explanation should be added to the definition of R&D as follows:

Following activities are excluded from the ambit/scope of the term ‘research and development’: audit, service evaluation, quality assurance, quality control and the like.

e. Definition of “medical emergency” needed;

New definition of ‘medical emergency’ proposed as follows:

Medical emergency means the sudden onset of a medical condition that manifests itself by symptoms of sufficientseverity, including severe pain, that the absence of immediate medical attention could reasonably be expectedby a prudent layperson who possesses an average knowledge of health and medicine to result in

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

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

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

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

f. Definition of “public health emergency” needed;

New definition of “public health emergencies” proposed:

Public health emergencies means a situation whose health consequences have the potential to overwhelmroutine community capabilities to address them. It focuses on situations whose scale, timing, or unpredictabilitythreatens to overwhelm routine capabilities.

3. Amendment of Clause 4

   Based on sub-clause 16 (1), Clauses 4 be modified as follows:

   Every data fiduciary shall process personal data of a person in such manner that protects the rights of, and is in the best interests of, the person. No personal data shall be processed by any data fiduciary **or data processor (instead of any person),** except for any specific, clear and lawful purpose.

4. Clauses (6) & (7)

   Comments:

   a. Clauses 6 & 7 which are about collection of personal data should precede clause 4, which is about processing, and therefore be rearranged and renumbered accordingly.
   b. Clause 6 should be modified by adding the word “adequate, relevant” as shown below:

   Revised clause 6:

   The personal data shall be collected only to the extent that is **adequate, relevant and** necessary for the purposes of processing of such personal data.

   Further modify clause 6 to add second sentence as follows:

   The personal data shall be collected only to the extent that is adequate, relevant and necessary for the purposes of processing of such personal data. **Personal data shall be kept in a form that permits identification of data principals for no longer than is necessary for the purposes for which the personal data is processed.**

   Comment:

The above change is needed to impart greater clarity and precision to the **principle of data minimisation.**

5. Modification of Clause 5.(b)

Comment:

It is recommended that the concept of a **reasonable person** be substituted in place of what a **particular data principal would reasonably expect**. The former concept has a clear standard in law whereas the reasonable expectation of 'the data principal' points to a particular person, which makes it a very difficult proposition to determine.

It is recommended that sub-clause 5.(b) may be reworded as follows:

Revised sub-clause 5.(b):

for the purpose consented to by the data principal or which is incidental to or connected with such purpose, and which a reasonable person would 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.

It is recommended that the following explanation be addedat the end of Clause 5.(b):

Explanation: Clause 5(b) in so far as health data is concerned, it 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) To advance the delivery of patient centered medical care;

(b) To provide appropriate information to help guide medical decisions at the time and place of treatment;

(c) 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;

(d) 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;

(e) To facilitate health and clinical research and health care quality;

(f) To promote early detection, prevention, and management of chronic diseases;

(g) To carry out public health research, review and analysis, and policy formulation;

(h) To undertake academic research and other related purposes.

Provided further that for public health related purposes mentioned in clauses (d) to (h) above, only de-identified or anonymized data shall be used, in the manner as may be prescribed by regulations.

6. Amendment proposed to sub-clause 7.(1)

   Comment:

   Replace the phrase ‘not collected from the data principal by collected from a third party as follows:

   Revised sub-clause 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 **collected from a third party**, as soon as reasonably practicable, containing the following information, namely:

7. Amendment proposed to sub-clause 7.(1)(e)

   Comment:

   It is suggested that the above may be modified as follows: Revised sub-clause 7.(1)(e) the basis for such processing, and the consequences, **if any**, 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;

8. Sub-clause 7.(1)(h)

Comment

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;

9. Amendment proposed to sub-clause 7.(2)

   Comment:

   Add the words ‘accessible, visible’ are especially relevant in cases such as cctv cameras monitoring public spaces.

   This may be done as follows:

   Revised sub-clause 7.(2):

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

10. Sub-clause 7.(3) be modified as follows:

    The provisions of subsections (1) & (2) shall not apply where such notice substantially prejudices the purpose of processing of personal data under section 12.

11. Clause 9(2) be modified as follows:

    Notwithstanding anything contained in sub-section (1),

    a) the personal data may be retained for a longer period if

       (i) explicitly consented to by the data principal, or necessary to comply with any obligation under any law for the time being in force, or

       (ii) it is health data, including biometric and genetic data, it shall be retained for the lifetime of the data principal concerned for provision of health services, and even longer, if required, 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.

12. Sub-clause 9.(3) be modified as follows

    Keeping in view the revisions of subsection (2) above, the data fiduciary shall undertake periodic review to determine whether it is necessary to retain the personal data in its possession.

13. Sub-clause 11.(6) be modified by adding a sentence as follows:

    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. **However, a data principal shall not be denied any health services merely because consent for processing of any personal information has been withdrawn.**

14. Sub-clause 12.(b) be modified by adding the highlighted phrase as follows:

    Under any law for the time being in force made by the Parliament or any State Legislature to **achieve legitimate interest and proportionate to the aim sought to be achieved.**

15. Sub-clause 12.(e) be modified as follows:

    to respond to any public health emergency, including undertaking 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;

16. New sub-clause 12(g) to be added as follows:

    To undertake

    (i) *per se* telemedicine, telehealth, e-health, m-health, digital health, or connected health services; or

(ii) any clinical research, public health research, scientific or historical research, research and development for innovation, archival, epidemiological or statistical purposes.

17. Clause 14 be modified as follows:

Revised sub-clause 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 specified in sub-section 14.(2) and as may be further elaborated by** regulations, after taking into consideration—

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

(a) prevention and detection of any unlawful activity including fraud, **nationally or internationally;**

(b) whistle blowing;

(c) mergers and acquisitions;

(d) network and information security, **including investigation and prosecution of cyber crime;**

(e) credit scoring;

(f) recovery of debt;

(g) processing of publicly available personal data; and

(h) the operation of search engines, and

(i) **tax information exchange arrangement with other countries.**

18. In sub-clause 17.(1) add the phrase ‘or surrogate as may be prescribed by regulations’ as follows:

Revised sub-clause 17.(1): The data principal, **or surrogate as may be prescribed by regulations’**, shall…

19. In sub-clause 17.(1)(b) replace the word ‘summary’ by ‘part’ as follows:

    Revised sub-clause 17.(1)(b): **a copy or extract of** the personal data of the data principal being processed or that has been processed by the data fiduciary, or any **part** thereof;

20. Sub-clause 17.(1)(c) be modified by deleting the word brief before summary as follows:

    Revised sub-clause 17.(1)(c): a 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.

21. Sub-clause 17(2) be modified as follows:

    The data fiduciary shall provide the information under sub-section 17.(1) to the data principal in a clear, concise, **transparent, intelligible, easily accessible form, using clear and plain language (in which it was processed) which is** easily comprehensible to a reasonable person.

22. Since the right to access has not been defined, clause 17.(3) is ambiguous and, therefore, needs to be modified as follows:

    Revised sub-clause 17.(3):

    The data principal shall have the right to **access online and retrieve/extract/copy relevant information, 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.

    Comment: It is not clear what the phrase ‘at one place’ implies. Does it mean at one physical location or does it mean at one online location.

23. After sub-clause 18.(1)(d) a proviso be added as follows:

Provided that health data, including biometric and genetic data, cannot be deleted as it shall be retained at least for the lifetime of the data principal or longer if required for clinical research, public health research, scientific and historical research, research and development for innovation, innovations in telemedicine, telehealth, e-health, m-health, digital health, or connected health services, archival, epidemiological or statistical purposes.

Comment: A patient's demand for deletion of his smoking history under S. 18.(1)(d) or of his entire health record in a hospital or a central health data repository cannot be accepted.

24. Sub-clause 18.(3) is very ambiguous. It is not clear what is intended by the phrase '...to indicate, alongside the relevant personal data, that the same is disputed by the data principal'. Does the data fiduciary have to annotate the relevant personal data or is something else meant? If so what?

25. Add a new clause 18.(5) as follows:

Data processor shall assist the data fiduciary to carry out requests for correction or erasure, where necessary.

26. A citizen/patient cannot be given the right to be forgotten made available under clause 20 of the PDP bill as far as health data is concerned. It is often impossible to conclude with certainty, perhaps until time has passed or tests have been done, whether a patient is suffering from a particular condition. An initial diagnosis (or informed opinion) may prove to be incorrect after more extensive examination or further tests. Individuals may want the initial diagnosis to be deleted on the grounds that it was, or proved to be, inaccurate. However, if the patient's records accurately reflect the doctor's diagnosis at the time, the records are not inaccurate, because they accurately reflect a particular doctor's opinion at a particular time. Moreover, the record of the doctor's initial diagnosis may help those treating the patient later.

27. A second proviso be added under sub-clause 20.(2) as follows:

Provided that no order shall be made under this sub-section:

(i) 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; **or**

(ii) if it is health data and its processing is necessary for public health purposes in the public interest (e.g., protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or if the processing is necessary for the purposes of preventative or occupational medicine (e.g., where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g., a health professional).

28. Sub-clause 21(1) may be modified 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 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 promptly acknowledge the receipt of such request within such period as may be specified by regulations.

    Notwithstanding the process prescribed in sub-section 21.(1), in case of a medical/public health emergency, the data fiduciary shall immediately release the necessary information in full or part, as may be requested by the data principal or surrogate, as may be prescribed by sectoral regulations or codes of practice.

29. The proviso of sub-clause 21.(2) may be modified as follows:

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

30. Sub-clause 22. (1)(d) be reworded as follows: the legitimate **business interests of the data fiduciary, including research and development for** innovation, is achieved without compromising privacy interests;

31. Sub-clause 24.(1) be modified as follows:

    Every data fiduciary and the data processor shall, having regard to the nature, scope, **context** and purpose of processing personal data, **proactively assess** the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, implement **and verify** the necessary security safeguards, including—

32. Add a sentence to subclause 25. (1) as follows:

    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.

    Provided that a breach may not need to be reported if the personal data was duly encrypted according to prevailing standards as may be prescribed by regulation.

33. 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.**

34. Modify sub-clause 25.(7) as follows:

    The Authority **shall**, in addition, also post the details of the personal data breach on its website.

35. Modify sub-clause 31.(3) as follows:

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

36. Modify clause 38 as follows:

    Where the processing of personal data is necessary for **clinical research, public health research, scientific or historical research, research and development for innovation, innovations in telemedicine, telehealth, e-**

health, m-health, digital health, or connected health services, archiving, epidemiological 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;

(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 undersection 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

(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 **clinical research, public health research, scientific or historical research, research and development for innovation, innovations in telemedicine, telehealth, e-health, m-health, digital health, or connected health services, archiving, epidemiological or** statistical purposes from the application of any of the provisions of this Act as may be specified by regulations.

37. Modify clause 40.(1) by shifting the phrase ‘in public interest’ as follows:

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

38. 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.

39. Sub-clause 49.(1) be modified as follows:

    It shall be the duty of the Authority to protect the interests **related to privacy** of data principals, prevent any misuse of personal data, ensure compliance with the provisions of this Act, and promote awareness about data protection.

40. Sub-clause 49.(2)(e) be modified as follows:

    issuance of a certificate of registration to data auditors and renewal, withdrawal, suspension or cancellation thereof and maintaining an **up-to-date** database of registered data auditors and specifying the qualifications, code of conduct, practical training and functions to be performed by such data auditors;

41. Sub-clause 53.(7) be modified as follows:

    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. **In case of health data, the inquiry officer shall allow a copy of all or any personal data to be retained by the data fiduciary or data processor for enabling continuity of care of the person or for any purpose referred to in Section 38.**

42. Sub-clause 55.(1) be modified as follows:

    Where in the course of inquiry under section 53, the Inquiry Officer has reasonable ground to believe that any books, registers, documents, records or data belonging to any person as mentioned therein, are likely to be tampered with, altered, mutilated, manufactured, falsified or destroyed, the Inquiry Officer may make an application to such designated court, as may be notified by the CentralGovernment, for an order for the seizure of such books, registers, documents, records **and any data in their custody or power**.

43. Sub-clause 55.(3)(c) be modified as follows:

to seize books, registers, documents, records **and any data in their custody or power**, it considers necessary for the purposes of the inquiry.

44. Sub-clause 55.(4) be modified as follows:

    The Inquiry Officer shall keep in its custody the books, registers, documents, records **and any data in their custody or power** seized under this section for such period not later than the conclusion of the inquiry as it considers necessary and thereafter shall return the same to the person, from whose custody or power they were seized and inform the designated court of such return.

45. Clause 58 be modified as follows:

    Where, any data fiduciary, without any reasonable explanation, fails to comply with any request made by a data principal under Chapter V, such data fiduciary shall be liable to a penalty of **at least** five thousand rupees for each day during which such default continues, subject to a maximum of ten lakh rupees in case of significant data fiduciaries and five lakh rupees in other cases.

46. Clause 59 be modified as follows:

    If any data fiduciary, who is required under this Act, or the rules or regulations made thereunder, to furnish any report, return or information to the Authority, fails to furnish the same, then such data fiduciary shall be liable to penalty which shall be **at least** ten thousand rupees for each day during which such default continues, subject to a maximum of twenty lakh rupees in case of significant data fiduciaries and five lakh rupees in other cases.

47. Clause 62.(3)be modified as follows:

    The Adjudicating Officers shall be persons of ability, integrity and standing, and must have specialised knowledge **competencies, skills and experience of, and not less than seven 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.**

48. Clause 68.(1)(b) be modified as follows:

in the case of a member, has held the post of Secretary to the Government of India or any equivalent post in the Central Government for a period of not less than two years or a person **of ability, integrity and standing, who has the 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.**

49. Sub-clause 82.(2) be modified as follows:

Nothing contained in sub-section (1) shall render any such person liable to any punishment under this section, if he proves that—

(a) the personal data belongs to the person, **or a blood relative of the person concerned**, charged with the offence under sub-section (1); or

(b) **personal data belongs to the person for whom he is a surrogate or guardian; or**

(c) 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, or

(d) **the re-identification was necessary for provision of health care services, or for processing personal data for purposes listed in Section 38.(1).**

Comment:

In relation to empowering clinical diagnosis of diseases and clinical discovery of disease mechanisms, and possible therapies, there are several scenarios where the absence of a re-identification method such as a unique identifier, of data or samples potentially put patients at risk. There is a risk of not reaching scientific objectives in research projects, because data cannot be connected on an individual patient level. Not reaching clinical studies objectives because of insufficient scientific evidence may also put patients at risk by prolonging the period for diagnosis and the options for treatment. Data sets of different experiments and samples of the same patients are held by different research organizations such as samples held at a biobank of university X, clinical or

genetic data from a natural history study or registry with hospital Y and biomarker data with research lab Z. Having different organizations involved, including cross border, is a common situation in clinical research for rare diseases. To fully exploit unanticipated, out-of-the normal signals in the biomarker results, the researcher (z) would need to have access to clinical and genetic data (y) of a particular participant from the hospital Y and be in a position to request another sample (x) of the same participant from the biorepository X. In the absence of a re-identification method such as a unique identifier, this research question may remain unanswered. Alternatively, the research needs to be re-done that may not be feasible based on costs and participant/sample availability without access to shared data and resources across borders. In addition, feeding back individual-level results to participants or inclusion in follow-up research may be impossible without a secure way of re-identification.

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5110051/

50. Sub-clause 94.(o) be modified as follows:

the provisions of the Act and the class of **clinical research, public health research, scientific or historical research, research and development for innovation, innovations in telemedicine, telehealth, e-health, m-health, digital health, or connected health services, archiving, epidemiological or** statistical purposes which may be exempted under section 38;

---------- ----------

For any queries or clarifications, contact:
Dr. Guriqbal Singh Jaiya MBBS, IAS, LLB
DHIndia Association, India
Email: gsjaiya@gmail.com