21 September 2020

To The
Ministry of Health and Family Welfare,
Government of India

Dear Sir,

Subject: Asia Internet Coalition ("AIC") Submission National Digital Health Mission: Health Data Management Policy

The Asia Internet Coalition ("AIC") and its members express our sincere gratitude to the Government of India for the opportunity to submit comments on National Digital Health Mission: Health Data Management Policy ("NDHE or Draft Policy").

The AIC is an industry association composed of leading Internet and technology companies. AIC seeks to promote the understanding and resolution of Internet and ICT policy issues in the Asia Pacific region. Our members are Airbnb, Amazon, Apple, Cloudflare, Expedia Group, Facebook, Google, SAP, Grab, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Verizon Media), and Booking.com.

First and foremost, we commend the Government of India's initiative on progressing the National Digital Health Ecosystem. We believe this is indeed a first step in realising the "Security and Privacy by Design" for the protection of individuals' data privacy. It certainly acts as a guidance document across the NDHE and sets out the minimum standard for data privacy protection that should be followed across the board in order to ensure compliance with relevant and applicable laws, rules and regulations.

We are also grateful to the Government of India for upholding a transparent, multi-stakeholder approach in developing this Policy. As such, please find **appended** to this letter, **detailed comments and recommendations** which we would like the Ministry of Health and Family Welfare ("**MoHFW**") **to consider** when preparing the Draft Policy .

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact us directly at Secretariat@aicasia.org or +65 8739 1490. Thank you for your time and consideration.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Detailed Comments and Recommendations

---

1. Breach notification:

The Draft Policy provisions for a breach notification requirement as a requirement for any breach with no defined levels of risk or number of records impacted. This is generally far exceeding the scope of most breach notification laws, and we would suggest alteration and aligning the breach notification requirements with other breach notification standards such as GDPR in the European Union.

We submit that the instances of a Data Breach Notification should be properly scoped and defined. We, thus, propose the following:

a) Limit the application of the reporting requirement to breach of "Sensitive Personal Information". We submit that: (i) the duty to report breaches should, thus, be limited to breaches of such Sensitive Personal Information only; and (ii) the portion of the provision making it mandatory to report breaches of information which may be used for "identity theft," as well as breaches of "other information" should be deleted.

b) The impact of the Data Breach should also be considered: We submit that the trigger for a legal requirement to notify in the event of a Data Breach, should be based on the materiality and the possible impact of the breach to the Data Subjects, i.e., include the requirement of significant or serious harm to warrant reporting. Applying a "significant harm" or "serious harm" threshold to breach notifications helps to ensure regulators have visibility into the incidents that pose actual risk to users and ensures regulators will be able to focus guidance and oversight activities where they are most needed. Removing the standard could result in over-notification. (Within the first nine months after the GDPR took effect, 64,684 data breach notifications were made to EU DPAs).

c) Further, the timeline for notification should be stated as "without undue delay" after becoming aware of the breach instead of within a 72-hour timeframe. Requiring notifications on short timelines can delay a company's efforts to investigate and stop the data breach, as well as interfere with ongoing law enforcement investigations.

d) The determination of whether there is a Data Breach belongs to the Personal Information Controller, should be consistent with existing international laws and rules. Pertinently, the GDPR and other foreign regulations, such as the U.S. Health Insurance Portability and Accountability Act (HIPAA) both place the responsibility to determine and report a Data Breach on a Personal Information Controller.

2. **Definition of health data**

Definition of health data will be very important in the Personal Data Protection Bill (PDPB), which is still under discussions. If health data is *sensitive* then it will be needed to keep a mirrored copy in India under the new PDPB, even if that isn't defined in the draft policy. If health data is *critical*, it will be needed to fully localize all copies and processing, which would be an onerous obligation.

We therefore recommend for a scoping of how health data should be considered for certainty, and should be considered *sensitive.*

3. **Storage**

The implications here should be about which level (i.e. Federal; state; individual hospital) determines how the data is stored/processed and with what provider. However, information about such levels is not explicitly mentioned in the draft policy and could be read as though each data set has to be stored by those entities in a way that implies in country only.

4. **Broad Definition of biometric data**

The definition of biometric data, which "means facial image, fingerprint scans, 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" is ambiguous, potentially stymying widespread use of important privacy-protecting innovations in healthcare. In this context, biometric data is not being used to identify data subjects, but to develop tools that can help diagnose disease. We suggest clarifying the definition and/or enacting explicit de-identification standards for biometric data being used to advance healthcare.

5. **Additional comments:**

- The Draft Policy claims to address technological and logistical challenges in Healthcare space in India, however the real intent seems to be to collect personal information and not too much focussed on committing universal and free healthcare to Indians.

- As the PDP bill already covers the concept of 'sensitive personal data', we suggest to refrain from any additional policy measures to protect the same. The Policy borrows the definition from the current text of the PDP Bill. As per the Policy, 'sensitive personal data' of patients including financial information (bank account and payment instrument details); physical, physiological and mental health data; and sexual orientation; genetic data; caste or tribe; and 'religious or political belief or affiliation'.

The Policy also lacks clarity on its relationship and alignment with the PDP bill, thus creating confusion and uncertainty. In the absence of a data privacy legislation, the Policy raises more concerns about the implementation and data privacy aspects.

- In addition to ISO 27001,we recommend that ISO 27018 should be mandate. ISO 27018 is a "Code of practice for protection of personally identifiable information (PII) in public clouds, acting as PII processors." This standard focuses primarily on security controls for public cloud service providers acting as PII processors.

- The usage of the Aadhaar ID has been restricted by the Supreme Court, however this Policy tries to link Aadhaar ID to the new health ID thus potentially violating the SC ruling.

- The Policy does not clarify the events under which the Government may seek access to the health record, thus raising law enforcement access concerns.

- The Policy states that if the storage of the personal data for a certain period of time is mandated by law, it cannot be erased; personal data may be blocked/ restricted, rather than erased, if law prohibits erasure. The Draft Policy needs to clarify that such obligation needs to be on the data controllers, and not data processors. Therefore, distinction between a data controller vis-a-vis a data processor is required. The obligations under para 14 should be on the data controllers.

- The Draft Policy requires the data fiduciary to conduct intrusive checks on the systems of the data processor. We recommend having more clarity on this. Will this mandate a physical audit of the data centers? We would like to reiterate that the prescribed ISO or other certification standards should suffice.