May 25, 2022

To
Dr. R.S. Sharma,
Chief Executive Officer,
National Health Authority,
9th Floor, Tower-1, Jeevan Bharti Building,
Connaught Place,
New Delhi – 110001

Subject: Inputs from Amazon Web Services on the Draft Health Data Management Policy 2022 (Policy)

Dear Sir,

We are grateful for the opportunity to provide feedback on the Draft 'Heath Data Management (HDM) Policy'. Achieving the objectives under the Ayushman Bharat Digital Mission (ABDM) requires a well-architected HDM policy to enhance user trust, drive innovations, and contribute to an integrated healthcare ecosystem in India. AWS therefore supports the vision to ensure that the health data of citizens is processed in accordance with the necessary data protection standards.

As you are aware, AWS's commitment to India is long term and substantive. Since 2016, we have set up the first AWS Region (consisting of multiple clusters of data centers) in Mumbai and have the second AWS region coming up in Telangana. Since December 2017, AWS has been a Ministry of Electronics and Information Technology (MeitY) empaneled cloud service provider in India. We have had the opportunity to support the Government on various projects that leverage public digital platforms to deliver population scale impact including the Common Services Centre (CSCs), e-Sanjeevani, that now serve as use-case for other governments to learn from and adopt. There are several instances where AWS teams have worked closely with hospitals and organizations across the healthcare value chain, in India and globally. Such partnerships are allowing healthcare service providers develop and test new services for their customers quickly, at scale to meet large demand with agility while minimizing IT costs. For instance, we are partners of the largest health administrative network in the United States, wherein AWS's cloud technology enables processing claims, pharmacy requests, and other health administrative functions, while maintaining full compliance with healthcare industry regulations such as The Health Insurance Portability and Accountability Act of 1996.

Our **key recommendations** on select high priority areas are summarized below for your kind perusal.

- **Narrow the applicability of the Policy and definition of 'sensitive personal data'** to Sensitive Personal Data (SPD) in the context of health, including health conditions and treatments of the data principal, Electronic Medical Records (EMR), Electronic Health Record (EHR) and Personal Health Record (PHR), for clarity.
- **Data Management for Data Processors, Training Audit and Termination of Contract** wherein we suggest the Policy rely on contractual arrangement between Data Fiduciary (DF) and Data Processor (DP) to enforce compliance obligations based on the requirements.
- **Enable compliance by** recognizing the sufficiency of the existing international standards and certifications and associated audits conducted for these certifications.
- **Aligning the Policy with the awaited Data Protection Bill 2021** (**DP Bill**) is critical to avoid overlaps and inconsistent regulations. NHA will be the sectoral regulator of health data, and this Policy must clarify how it will align itself with the DP Bill once it becomes a law. Further, we suggest that the NHA should delete reference to non-personal data till the government has decided on the matter.
- **Remove uncertainty by adopting a risk-based approach** for data breach and non-compliance**.**
- **Remove data localization mandates for personal data** as a whole. The Policy should have a focused definition of health data, instead of extending its scope to all personal data collected by entities in the

ABDM ecosystem. Smooth data flows across healthcare systems with safeguards is necessary for improved care delivery, efficient research, lower development costs, facilitating diagnosis and treatment.

We thank you for including additional ground of processing of data in medical emergency situations, or based on the order of a competent court in the draft provision. Health data processing in emergency situations requires a seamless process, this needs further deliberation on enabling mechanisms.

Our detailed response is enclosed in Annexure I for your consideration. We would be happy to respond to any questions or requests for additional information.

We look forward to continued interactions to support with framing guidelines, capacity building programs, etc.

Best Regards

Yours Sincerely

Head- Public Policy for AWS – India/South Asia
Email: bishakha@amazon.com
Mobile: +91-9873100040

INPUTS TO THE DRAFT HEALTH DATA MANAGEMENT POLICY, 2022

Cloud services, such as those offered by AWS, can help the achieve objectives of the ABDM to develop the essential supporting the integrated digital health infrastructure of the country, and help the National Health Authority and healthcare service providers to optimize their relationship with technology, enable rapid innovation, automate and strengthen security, improve customer experience, and lower costs.

We thereby submit our recommendations to further refine this essential policy:

I. **Narrowing the applicability of the Policy and definition of 'sensitive personal data' (SPD):** The Policy has adopted the definition of 'sensitive personal data' as described in the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (SPDI Rules) (Rule 3),[1] without addressing what types of "health data" will be considered SPD. The scope of the definition under the SDPI Rules is quite broad in comparison to the Policy, which is concerned with only health-related data. The Policy should therefore provide a clear scope of the types of data that would be considered sensitive and articulate the appropriate safeguards for each type. Reproducing the entire list of proposed SPD categories from the SDPI Rules could lead to significant confusion for the data principals, DFs and DPs trying to comply with the Policy. It also goes against the 'purpose limitation' principle discussed in the Policy (Paragraph 26.5), i.e., the purposes of processing personal data would be limited to the purposes defined by the NHA (Paragraph 9.3; and 26.5). As a result, while the Policy is intended to apply to health-related data only, such broad language may result in Policy becoming applicable to all categories of SPD and personal data. This may have unforeseen implications of impacting the treatment of such data in non-health related contexts. Such a broad scope would also make the Policy applicable to all health service providers, who may or may not deal with sensitive health data. This Policy is a sector-specific policy, and it must restrict its applicability to the collection, processing, storage, sharing or retention of ABDM data.

   Recommendation: Therefore, we recommend that the proposed definition of SPD be narrowed by providing clarity on the types of data that would constitute SPD, including health conditions and treatments of the data principal, EMR, EHR and PHR and restricting the scope of personal data and SPD to only health-related data points.

II. **Data Management for Data Processors, Training Audit and Termination of Contract:** The Policy mandates that DFs place extensive obligations on DPs with respect to handling of data and their internal processes. While we note that the DF must maintain responsibility with respect to the compliance of the DP while carrying out activities on its behalf so as to protect the individuals to which the personal data and SPD pertain, certain obligations may amount to an overreach into management of the DP's activities. The Policy requires that the agreements between DPs and DFs must be renewed on a periodic basis, rather than as per the needs of the entities (Paragraph 27.2(c)). Similarly, under the Policy, DPs are required to comply with the 'same level of data protection' adhered to by the DF (Paragraph 27.2(d)). Such requirements will result in high costs for both DPs and DFs, in terms of their compliance and manpower costs, service pricing and ease of business. A better alternative to this could be to leave these concerns to the contractual arrangements between DFs and DPs.

   The Policy mandates data fiduciaries to (i) develop training and awareness materials around data protection and privacy; their employees and for data processors; (ii) develop role-based training for individuals or teams considering the nature of processing/ their role; and (iii) conduct periodic (at a minimum, on an annual basis) training and awareness programs, for all employees and DPs (Paragraph 27.2(h)). This is overly prescriptive, and not necessarily an area of core competence for the DF.

[1] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

Recommendations:
(i) Therefore, we recommend that the Policy should rely on DPs and DFs to decide and share responsibilities through contractual mechanisms. This will be facilitated by paring down the obligations that would otherwise overburden DFs and DPs, such as removing Para 27.2(c) of the Policy and. Further, Para 27.2(d) should be pared down to require contractual enforcement of the applicable law on DPs.

(ii) We recommend that DFs should be given the flexibility to pre-qualify training programs required (by DPs) to meet their requirements on data privacy. Further, to provide guidance to DFs when appointing or outsourcing to DPs that are technology service providers, including CSPs, we recommend providing some further clarity including referencing international standards such as ISO 270018 and System and Organization Controls (SOC 2) Privacy Type I Reports. We also recommend that the requirement to re-train DPs on an annual basis should be removed. This will not only ease the burden on the DF but also on the DP, whose team may be required to attend similar training programs for multiple vendors.

III. **Enabling compliance with existing international standards and auditing requirements:** The Policy imposes certain requirements in relation to auditing and compliance with standards in relation to processing of health data. For example, the Policy requires DFs to implement necessary security safeguards such as use of de-identification and encryption methods, prevent misuse/ unauthorized access to personal data, etc., (Paragraph 27.1.(c)). The DF also needs to undertake a review of its security safeguards periodically (Paragraph 27.1.(c)).

The Policy also imposes the following auditing requirements- (a) the security standards implemented by the DF should be audited at least once a year by an independent auditor approved by the central government (Paragraph 27.1(d)), and (b) the DFs must conduct a periodic audit to ensure that the DPs are processing personal data in compliance with the Policy (Paragraph 27.5.(b)). DFs are mandated to engage DPs to act on their behalf through a valid contract (Paragraph 27.2.(b)). While the DPs implement necessary security measures for all data hosted by them, they take specific measures based on the DF's instructions. Additionally, there are multiple instruments that provide for auditing requirements of security controls expected to be implemented by DFs/DPs. Some examples are MeitY's requirements for the empanelment of Cloud Service Providers (CSPs)[2] and the forthcoming DP Bill.

Recommendations:
(i) The Policy must recognize the sufficiency of the existing international and national standards and certifications for auditing and provides for an exemption to the entities who are already meeting such international and national standards. With the intention to create a business-friendly approach, the Policy may remove references to specific standards and instead allow businesses to choose appropriate standards to apply to their business, based on their security and other requirements. This will ensure that there is no duplication or unnecessary compliance and/ or cost burden on the stakeholders' subject to the Policy. Alternatively, empaneled auditors should be authorized to conduct an annual audit for various data-protection related standards.

(ii) Further, the Policy must clarify that audit related obligations of a DF should not be passed on to a DP. Instead, DPs can seek information from the DF, for example, about security safeguards, as per the contractual agreement between them, but it is the primary responsibility of the DF to provide the required information for its audit.

IV. **Processing of data and alignment with DP Bill:** We commend the NHA for including provisions that allow non-consent-based processing and allowing the processing of data in emergency situations, such as in a medical emergency or threat to life, or public health, or based on the order of a competent court (Paragraph 13.5).

[2] MeitY's requirements for the empanelment of cloud service offerings of Cloud Service Providers.

That said, concerns about the overall alignment of the Policy with the DP Bill persist. One of the objectives of the Policy is to ensure secure processing of personal data and SPD 'in compliance with all applicable laws' (Paragraph 3(a)). While many privacy and data protection principles in the Policy are based on provisions of the DP Bill, the Policy differs on certain aspects from the DP Bill.

The Policy requires DFs to obtain fresh consent in case of changes to its policy or procedures, or if there is a new purpose of processing of data. It introduces certain new requirements which are not given in the DP Bill. These include the creation of a 'consent artefact' (Paragraph 11.5) and the requirement for DFs and DPs to comply with data retention and archival guidelines to be notified from time to time.

Inconsistencies between the Policy and the DP Bill may create confusion about the requirements to be met under the applicable laws, which will impact all DFs and DPs handling personal data under the Policy. They will need to set up different systems and checks, depending on whether their use will fall under the Policy or the DP Bill. Such a requirement of evaluating the standard to be met on each occasion is highly time consuming and resource intensive and will not be viable for most players.

Further, the Policy seems to suggest that the NHA will devise a procedure for granting access to anonymized or deidentified data under the Policy (Paragraph 29.2). However, there are multiple other developments underway for non-personal data (NPD) regulation such as (i) the MeitY-appointed Committee of Experts (CoE) for NPD which recently released its report[3] and concluded its public consultation process; (ii) the Draft India Data Accessibility and Use Policy, 2022[4] which provides a framework for intergovernmental NPD sharing; and (iii) the DP Bill, which in its current form includes NPD within its framework.

Any NPD-related provisions framed by the Ministry of Health and Family Welfare (MoHFW) should consider the concerns raised by stakeholders in response to the CoE's consultation process, such as adverse consequences of mandatory sharing of NPD, violation of associated intellectual property rights, risks to security and privacy of the data principal and disincentivizing innovation in data-related sectors. The MoHFW should avoid coming out with any provisions on non-personal health data or unaligned framework for non-personal health data and participate in ongoing deliberations.

Recommendation:
(i) We recommend that the NHA should clarify how it will align itself with the DP Bill once it becomes enforceable law. It should also clarify how the concerned parties should comply with the Policy in case there is a contradiction or an inconsistency with the DP Bill.

(ii) The NHA should not notify any rules on NPD at least till (a) the DP Bill has been passed; (b) the DPA has issued appropriate standards, rules and regulations on anonymisation; and (c) the CoE on NPD has concluded its deliberations and published its recommendations after inviting comments from all relevant stakeholders, including from the public.

V. **Removing uncertainty for ecosystem participants by adopting risk-based approach for data breach and non-compliance:** The Policy requires that data breaches be reported within time limits specified periodically by the NHA and the applicable laws (Paragraph 33.2). While DFs are responsible for responding to data breaches, DPs may be subject to these breach reporting and incident response obligations by virtue of data being stored or processed through their services.

[3] MEITY, Report by the Committee of Experts on Non-Personal Data Governance Framework 48-50 (2020).
[4] MEITY, draft India Data Accessibility and Use Policy, 2022.

Recommendation: We recommend a risk-based approach to reporting data breaches that allows sufficient time to assess and respond to the breach. This will allow for better response outcomes for organizations, who will be able to focus on damage limitation while enabling then to share quality information for incident analysis.

VI. **Removing data localization requirements for personal data:** The Policy requires all personal data to be stored within the geographical borders of India (Paragraph 26.6), which is a new addition in the Policy. Personal data in the Policy is defined as any data about or relating to a natural person who is directly or indirectly identifiable, having regard to characteristics, traits or any feature of the identity of the person. As the Policy applies to all entities in the ABDM ecosystem (all individuals with an ABHA number, healthcare professionals, governing bodies, research bodies, pharma sector entities, and all entities collecting or processing data, which will include services providers involved in the ABDM), any personal data they collect, which is not technically health data but incidental to such purposes, would also need to be localized in India.

This is excessive as even the draft DP Bill does not require localization of all personal data, mandating such provisions for only specific categories of data, namely SPD and CPD. Under the DP Bill, health data is SPD and would be stored within India.

Recommendation: The Policy should be aligned with the DP Bill and broad requirements for local storage of all personal data should be removed. It is our recommendation that health data be defined clearly such that any storage requirement be extended in accordance with the SPD and CPD local storage requirements under the DP Bill.

VII. **Privacy related provisions prescribed in the Policy:** There are two areas of concern outlined below.
(i) Consent in relation to collection and processing of personal data or SPD- The Policy provides for processing of personal data or SPD by DFs only after the consent of the data principal has been obtained (Paragraph 9.1). This is not aligned with comparable international frameworks in other jurisdictions, including the GDPR[5] which provides for additional grounds for processing, such as contractual necessity or legitimate interests. This inhibits many ordinary uses of personal data where its processing would clearly benefit the data subject. In these cases, the privacy risks are limited, the data principal could reasonably expect the processing, consent cannot be obtained, and data principals are unlikely to object to the processing. We recommend that these grounds be recognized under the Policy in addition to consent because obtaining valid, meaningful, and informed consent of data principals for every processing activity is technically onerous, and likely to impair the user interface and experience, without enhancing data protection outcomes, and may are likely to result in consent fatigue. This should also be aligned with section 12 of the DP Bill, and references to permissible grounds for non-consensual processing should be included.

Recommendation:
(i) The grounds for processing should be expanded to include (i) processing when it is necessary for the performance of a contract to which the data subject is a party; (ii) where the processing is necessary to protect the vital interests of the data subject; (iii) for legitimate interests such as fraud prevention; and (iv) ensuring the network and information security of an organization. We therefore recommend that the Policy explicitly allow for both express and implied consent, as well as allowing personal data to be processed on broader bases than just consent.

(ii) Any sharing of personal data by DF to Health Information Units (HIU) requires prior consent under the Policy (Paragraph 28.1). This could lead to consent and notification fatigue and we recommend expansion of grounds for processing without consent.

[5] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(ii) Privacy notice for collection of personal data and SPD- We note that the Policy requires the privacy notice to contain *inter alia* details of individuals/ entities along with their contact details, including other DFs or DPs with whom personal data may be shared (Paragraph 10.2(f)). It would be unduly burdensome for the DF to notify the data principal of all current or potential DPs to whom the DF will or may disclose the data, prior to collection. In any case, it is the DF's responsibility to ensure that the DP processes the data in accordance with its instructions and in consonance with the Policy. By requiring notification to data principals of such relationships, it places undue burden on these data principals to continually acknowledge notices intimating changes in DPs. This will result in consent fatigue for the data principals, without providing any additional protection to them. Additionally, the DP is accountable to the DF, and the DF to the data principal. There should be no direct relationship between the data principals and the DP handling their personal data and SPD. Furthermore, the Policy is unclear on whether this notice requirement would apply only to the third parties to whom the DFs are sure about disclosing the data principal's information at the point of collection, or whether it should include all potential future disclosures.

Recommendation: We therefore recommend that Paragraph 10.2(f) of the Policy be amended as follows: *"….**to the extent practical**, the individuals or entities along with their contact details, including other data fiduciaries ~~**or data processors**~~ with whom personal **or sensitive personal data** may be shared, if applicable.;"*

VIII. **General principles governing consent framework:** The Policy states that where consent is obtained via electronic means i.e., electronic consent, DFs should "make use of appropriate technological means to prevent security breaches" (Paragraph 8(b)). While we understand that consent obtained through electronic means should be done in a manner so as to ensure integrity, it is unclear why the Policy prescribes a different threshold for consent obtained through electronic means, with regard to security breaches. It should be the collection, storage or processing of personal data or SPD that is linked to "appropriate technological means", rather than the electronic consent. There could be scenarios where the data is collected via non-electronic methods, but later converted and stored in electronic formats. This has already been addressed under Paragraph 27.1 of the Policy and does not need to be duplicated here.

Recommendation: We therefore recommend the following amendments be made to paragraph 8(b) of the Policy: "*Specifically, in case of electronic consent, data fiduciaries should make use of appropriate technological means ~~**to prevent security breaches and**~~ to ~~**guarantee**~~ **ensure** integrity of access permissions given by data principals. Such technological means must be in conformance with the national and international standards, as may be applicable."*