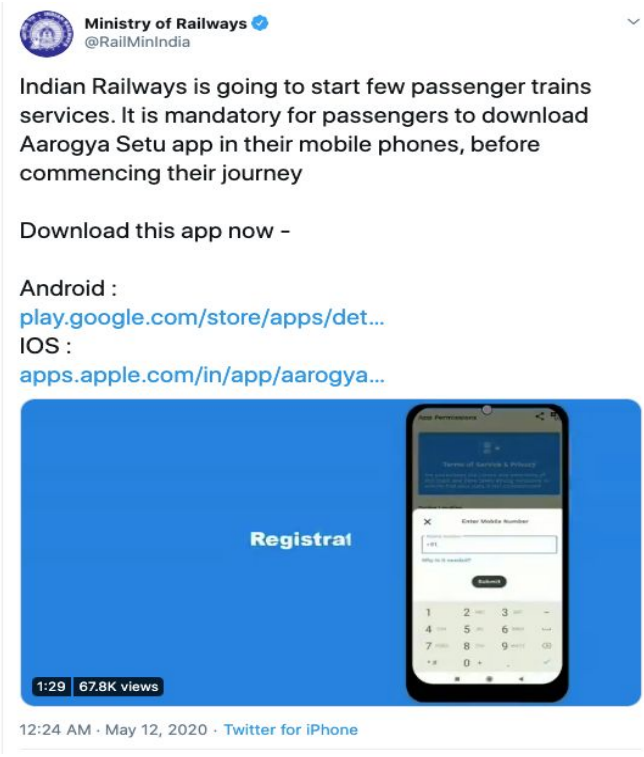
Summary and Analysis of "Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020"

1. The Ministry of Electronics and Information Technology, Government of India ("**MeITY"**), issued an Order No. 2(10)/2020-CLeS dated 11.05.2020 which notifies the "Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020" ("**Protocol**"). This document is meant to serve as a critical appraisal of this new Protocol. Towards the end of this document we also analyse certain disclosures on the Aarogya Setu app which were made during a press briefing dated May 11, 2020 by the Secretary of MeitY, Ajay Prakash Sawhney.

2. Our analysis also comes in the wake of the Aarogya Setu app being made mandatory to access many essential services and facilities. For instance, in a late night tweet, the Ministry of Railways announced that as passenger trains restart, it will be mandatory for passengers to download the app. Similarly, the Ministry of Civil Aviation has proposed a standard operating procedure (SOP) to restart commercial travel. The proposed SOP reportedly will require all flight passengers to have a "Green Status" on the Aarogya Setu app.



Fails to Satisfy the Legality Threshold

3. At the outset, it is stated that the Protocol **is not a statute, and nor does it offer any legislative foundation for the Aarogya Setu Mobile Application**. Therefore, the primary issue of Aarogya Setu lacking legal basis is still alive and unaddressed. For

clarity fundamental rights under the Constitution cannot be restricted by the Government even for legitimate purposes without express legislative authorisation. The Protocol is not - and does not purport to provide - any such authorisation. A troubling aspect in this regard, is that Government authorities have said that there are no plans to create an underlying legislation to hold the usage of the app accountable, since the "*priority at present is to deal with the epidemic itself*."

4. The idea of disregarding civil rights and the rule of law is deeply troubling and would not be acceptable even in emergency circumstances. This is demonstrated through the Hon'ble Supreme Court's observations in *KS Puttaswamy (Retd) and Anr v Union of India* [(2017) 10 SCC 1]. While recognising the right to privacy as a fundamental right, the Hon'ble Supreme Court observed that:

> "*An unauthorised parting of the medical records of an individual which have been furnished to a hospital will amount to an invasion of privacy. On the other hand, the* ***state may assert a legitimate interest in analysing data borne from hospital records to understand and deal with a public health epidemic****... to obviate a serious impact on the population.* ***If the State preserves the anonymity of the individual*** *it could* ***legitimately assert a valid state interest in the preservation of public health to design appropriate policy interventions***."

5. In the context of public health crises the Hon'ble Supreme Court in the right to privacy judgement observes that any curtailment or deprivation must take place **under a regime of law**. The Protocol clearly does not satisfy this threshold. Now let us analyse the Protocol itself keeping the inherent shortcoming of the lack of an underlying legislation and the above grounds in mind.

Authority to Issue Order

6. The Central Government has constituted several Empowered Groups under the Disaster Management Act 2005 ("**DMA 2005**"), *vide* Orders No. 40-3/2020-DM-I(A) dated 29.03.2020 and 01.05.2020. The mandate of these Empowered Groups is stated within the Protocol. It indicates this includes "*(identification) of problem areas and (providing) effective solutions therefore, delineate policy, formulate policy, formulate plans, strategise operations and take all necessary steps for effective and time-bound implementation of these plans / policies / strategies in relation to the Covid-19 pandemic.*"

7. **Questionable Legality of the Empowered Groups:** Powers have been delegated to these Empowered Groups in pursuance of the orders dated 29.03.2020 and 01.05.2020. The Order dated 29.03.2020 purportedly delegates such power under Sections 10(2)(h) and (i), by which the National Executive Committee constituted under the Disaster Management Act has powers to "*monitor, coordinate and give*

directions regarding the mitigation and preparedness measures to be taken by different Ministries or Departments and agencies of the Government" [10(2)(h)], and "*evaluate the preparedness at all governmental levels for the purpose of responding to any threatening disaster situation or disaster and give directions, where necessary, for enhancing such preparedness*" [10(2)(i)]. However, Section 10 does not permit any delegation of power — which is, however, permitted by Section 69. Even so, neither Section 10 nor Section 69 (and indeed any other provisions of the DMA 2005) contain any reference to an "Empowered Group". **Therefore, the legality of this delegation of power upon Empowered Groups is questionable**.

8. Keeping this questionable legality in mind, we notice that the Government has constituted 11 Empowered Groups. **Empowered Group 9 is specifically tasked with Technology and Data Management**. It is important to note that to the best of our knowledge there is no mention in a press bulletin, Government notification, the Aarogya Setu app's Terms of Service, Privacy Policy or FAQs, that Empowered Group 9 has been solely responsible for the creation and execution of the Aarogya Setu app.

9. A perusal of the contents of the Protocol dated 11.05.2020 reveals that this has not been stated therein as well. In addition, there is no reference in this Order or any other government notification about the means through which Empowered Group 9 has sought external inputs on the drafting of the Protocol. There is also no reference in this Order or any other government notification about the actual membership composition of Empowered Group 9 on Technology and Data Management.

10. It must also be noted that Recital 4 in this Order states that the functioning of the Aarogya Setu App "... ***relates to technology and data management and certain necessary steps*** *are required to be taken to ensure its effective operation to detect and mitigate the spread...*" of the COVID-19 infection, and enhance government preparedness at all levels. Recital 4 is drafted in a manner, which justifies the centralised collection of data through the new Aarogya Setu platform. It does this without any discussion about the choice of design, and why existing alternatives which exist through avenues like telecom operators, or for that matter anonymised mobility reports reports developed in an open source format by researchers and organisations like Facebook/Google, are not enough. **There is no discussion on why existing data at the Government's disposal collected through hospitals, the Indian Council of Medical Research, the Integrated Disease Surveillance Programme, on ground surveillance teams, etc. does not suffice in fulfilling the objective referenced by Recital 4**.

11. The recitals/preamble of the Protocol also fail to acknowledge the fact that when data is collected in a primary fashion from individual users, it is of course a more intrusive collection process. Therefore it comes with inherent risks to informational

privacy. In this context, the preamble to the Protocol is insufficient as there is no reference to adhering to principles of minimisation, limitations, and the need to incorporate other safeguards.

Paras 1—3: "Rationale for this Protocol"

12. The Rationale for the Protocol is explained at length. It stresses on the need for *efficient* data collection and sharing. Unfortunately, there is little to no discussion on ensuring that the most privacy-respecting practices are adopted in this regard. The Protocol fails to refer to the vast data collection which the Government already has in place. It fails to acknowledge the data that is already collected by Governments from the hospitals and the shortcomings therein/incompleteness of this data in effectively responding to COVID-19. It therefore fails to demonstrate or even build a satisfactory case for the need for further data. Additionally, it does not highlight how this data collection will actually augment the Government's response in containing the novel coronavirus.

13. Keeping this in mind, the Protocol arbitrarily states that there is an urgent need for data pertaining to individuals "*to formulate appropriate health responses for addressing the Covid-19 pandemic*". It also states that currently governments are working to "*formulate appropriate health responses to not only contain the epidemic but also protect the health and safety of the community at large*".

14. The range of "Appropriate health responses" **is expansive and includes** "prevention and management of the Covid-19 pandemic, syndromic mapping, contact tracing, communication to an affected or at-risk individual's family and acquaintances, performance of statistical analysis, medical research, formulation of treatment plans or other medical and public health responses related to the redressal and management of the Covid-19 pandemic." In fact such an expansive definition is curious since a think tank which supported the Government of India in drafting the Protocol has stated in an explainer blog post that the purpose of the Protocol is "*exposure notification and contact tracing*". If that were indeed the case, then such a broad definition for Appropriate health responses is incompatible with the principle of *proportionality*.

15. In contrast, all other apps across the world's democracies (across the economic and geographical spectrum) are only deploying apps to support/expedite their country's on-ground contact tracing efforts. In India the app's expansiveness is being positioned as it speaks to India's innovation. This would be a disingenuous characterisation. Most other countries are taking their time to ensure that the application of such technologies when ultimately scaled are in fact consistent with their civil liberties obligations.

16. The Protocol defines the term "Individual" to **mean** "*persons who are infected, at high risk of being infected or who have come in contact with infected individuals.*" The

"Data" (referred to as response data) **includes** "*demographic data (name, mobile number, age, gender, profession and travel history), contact data, self assessment data and location data*".

17. The Rationale therefore confirms that: (i) The Central Government is amassing vast amounts of personal data from individuals; (ii) The Aarogya Setu App entails collection of sensitive personal data in a manner not being witnessed in other democratic states or through apps developed by the private sector; (iii) There is no specific mention of how data collected through the Aarogya Setu App adds to the data collection exercise already being conducted through other means by the Central Government, and; (iv) The purposes for which such vast amounts of data is being gathered through the Aarogya Setu App have not been strictly defined, and they go far beyond the immediate issue of identifying persons affected / at risk of being infected with Covid-19. **Therefore, the Protocol clearly supports a *prima facie* case that the government is engaging in excessive data collection and infringing the right to privacy. It is not engaging in this data collection through the least restrictive measure that is hemmed in by clear purpose-based requirements, and is, therefore, falling foul of the proportionality (see Para 4) principle.**

Para 4: "Implementation of this Protocol"

18. MeitY is designated as the agency responsible for implementing the Protocol. The National Informatics Centre ("**NIC**"), identified as the app's official developer, is mentioned as being responsible for collection, processing and managing response data collected by the Aarogya Setu App.

19. It is not specified anywhere how this Protocol will interact with the Aarogya Setu app's Terms of Service and Privacy Policy that were already in place. For instance, the Privacy Policy already contains a set of practices governing data collection and storage. Many of those provisions are now in conflict with the Protocol. However, the Protocol fails to outline the effect of these conflicts and how they will be rationalised. This creates confusion, uncertainty, and risks of greater flexibility for retention and sharing of people's personal and sensitive personal information.

20. Surprisingly, even though Empowered Group 9 is a specially constituted body with a restrictive mandate, the Protocol states that "*MeITY shall act under the overall direction of the Empowered Group 9" for purposes of this Protocol.*" Since Empowered Group 9 was set up by the National Executive Committee; and the chairperson of the National Executive Committee is the Union Home Secretary, we believe that the chain of command evokes concerns of possible mission creep. What is especially concerning is that India's public health institutions have minimal leadership even as these technologies are being built to respond to a public health crisis. This is again contrary to other countries where technology systems are being controlled and

operated by public health authorities. In fact they are providing reassurances to the public that datal not be shared with law enforcement authorities.

Para 5: "Principles for Collection and Processing of Response Data"

Purpose, Use and Processing of Data [5(a) to 5(c)]

21. The Protocol states that the Privacy Policy of the Aarogya Setu App must specify any response data collected by NIC and the purpose behind the same. This data collection must be "*necessary and proportionate*" to the formulation / implementation / improvement of appropriate health responses, and the data must be processed in a "*fair, transparent and non-discriminatory manner*".

22. The use of such phraseology is meant to demonstrate that the Protocol incorporates *purpose* and *use* limitations on data collected by the App. However, they are far from *restrictive*. As already shown above, "Appropriate health responses" is a broad term that covers a wide gamut of government operations. In other words, "purpose limitation" and the principles of necessity and proportionality with respect to data collection acts as a meaningful constraint only if the purpose is spelt out with clarity and specificity to start with. If the purpose itself is excessively broad, vague, and evolving, then "necessity" and "proportionality" have no meaning at all, since data collection needs to be necessary and proportionate with regard to the purpose for which it is being collected. The Protocol, therefore, attempts to do an end run around core data principles by leaving the purpose so vague and ill-defined, that excessive data collection can potentially always be justified as necessary and proportionate.

23. Further, the Protocol's reference to the principle for processing data in a "*fair, transparent and non-discriminatory manner*" rings hollow. Specifically, it does not require the NIC to *publicly share* its data processing practises. **In fact, one way for processing to be transparent is by publishing the app's underlying source code. Instead, India has not published the Aarogya Setu app's source code and even now, a recent statement of the Secretary, MeitY indicates a reticence to publish the source code before the public**.

24. As such there is a need for greater specificity in language to demonstrate fidelity with proportionality. Vagueness affords the Government greater scope to repurpose the app in pursuance of "improvement of health responses". We have already seen this with the introduction of new features within the app and with reports of plans to further expand its capabilities moving forward. Examples of greater specificity may be seen with Singapore's TraceTogether app. The Trace Together app's statement on "Privacy Safeguards" says that only Singapore's Ministry of Health may only use data collected by the app solely **for contact tracing of persons possibly exposed to COVID-19**. This shows the presence of singular explicitly defined

purpose, a key feature of the purpose limitation principle, which the Protocol fails to do.

Storage of Data [5(d) to 5(f)]

25. The Protocol states that response data is to be "securely stored" by the NIC and shared as per the Protocol. However, the Protocol does not elaborate upon what it means to securely store the data, and whether the same kinds of security standards or the safeguards which shall be followed for the different kinds of data gathered, shared and retained.

26. The Protocol requires a default setting that contact and location data remain on the device and not uploaded on to the server. This default setting is, however, immediately overridden by the next sentence which states that such data **may be** uploaded to the server to formulate / implement appropriate health responses. Given the breadth of this purpose, there is, in effect, no clarity or certainty on when contact and location data may be uploaded on the server. Moreover, the breadth of this exemption allows for the seamless creation of a centralised system, and affords the app's Privacy Policy enough scope to collect and export people's contact and location data. This is particularly concerning, because the Privacy Policy reveals that Aarogya Setu collects people's location data at `15 minute intervals.

27. As per the Protocol the **contact, location, and self assessment data** gathered by NIC "*shall not be retained beyond the period necessary to satisfy the purpose for which it is obtained*". This period "*shall not ordinarily extend beyond 180 days from the date on which it is collected, after which such data shall be permanently deleted*". For **demographic data** collected by NIC, the Protocol states that it shall be "*retained for as long as this Protocol remains in force or if the individual requests that it be deleted, for a maximum of 30 days from such request, whichever is earlier.*"

28. The storage policies adopted by the Protocol are highly deficient, and are clearly contrary to a proportionality-based approach to restricting people's fundamental right to privacy:

    A. Data retention for six months, without any process of review while allowing for potential extension of this time-limit, is not the least intrusive measure that could be adopted. This is because it allows for retaining of people's personal data for durations much beyond the duration of the Protocol itself. Consider the following example. Imagine someone's contact/location/self assessment data is exported on daya 45. Then that data could be retained for a period of 45 days beyond the purported last date of the Protocol which is fixed at 6 months *vide* Para 10, wherein this data retention takes place in a legal vacuum.

B. The Protocol also fails to clarify what are the *extraordinary* circumstances in which the Government may unilaterally retain contact, location and self assessment data for a period longer than 180 days.

C. There is no policy for destroying contact, location and self assessment data based on a user request, contrary to the Protocol for demographic data. The total failure to consider user-request based destruction of such data amounts to retaining personal data without consent and is a clear breach of the right to privacy. Of course the whole notion of the usage of the app being based on informed consent does not apply, when the usage of the app is being mandatory in many different essential facets.

D. Para 5(e) also fails to clarify whether this provision applies to anonymised data or not. This is important to highlight because the current Privacy Policy of the Aarogya Setu App specifies that the data retention clause is not applicable to anonymised data. **Such exemptions, if they still subsist, retain concerns of permanent systems of data analysis/surveillance**. **Any legal instrument must necessarily address the mechanism for destruction of the entire centralised and merely the deletion of personal data. Such measures are necessary to ensure people's privacy are not compromised after the initial purpose of any legitimate app has lapsed**.

E. The Protocol fails to clarify the means through which individuals can enforce data deletion requests as allowed under Para 5(e).

Para 6: "Principles for Sharing Response Data"

29. Para 5(f) states that response data may only be shared by the NIC, the government entity which maintains and operates the Government's central server, in accordance with provisions laid down in the Protocol. The sharing of data is delineated through Para 6.

30. The Protocol allows for sharing data containing personal information, as well as "de-identified" data that is stripped of such information and assigned a randomly generated ID [Para 6(b)] as well as requires the NIC to log the data sharing process [Para 6(c)].

31. However, the Protocol does not specify the process by which a random ID will be generated. It therefore does not expressly choos privacy-respecting dynamic ID systems. This has allowed the NIC to adopt a static ID system (which we see even in the Privacy Policy as well) which can lead to easily recovering the "stripped" personal data by matching the ID it with other identifiers. Further, the process does not specifically refer to "Hard Anonymisation" [*see*, Para 8] suggests that the random ID generation is not going to offer the privacy protections secured by this process.

32. Importantly, the data sharing process is also not the least intrusive alternative that is available. Para 6(c) states that the NIC must document data sharing "*to the extent possible*" and does not create a hard obligation. Further, the Protocol only requires a one-time logging by the NIC of when data is shared, without any time-limits on the data sharing process, or provisions for any periodic reviews by the NIC / MeITY of whether the data sharing is required to continue after expiry of a certain period of time. **None of this data-sharing is specified as being made known to the public, therefore creating a transparency gap and serious trust deficit. Thus, the Protocol demonstrates an overzealousness to ensure wide access to personal data with state actors with minimal accountability and transparency of the same.**

Data Shared

33. The Protocol allows **personal data i.e. response data** to be shared with the:

    i. Ministry of Health and Family Welfare, Government of India,
    ii. Departments of Health of the State / Union Territory Governments / Local Governments,
    iii. NDMA, SDMAs,
    iv. **Such other Ministries and Departments of the Government of India and state Governments** and
    v. Other public health institutes of the Government of India, State Governments and local governments".

34. That personal data can be shared with "*such other ministries and departments of the Government of India and state Governments*" creates a serious risk of government overreach. Specifically, such provision suffers from overbreadth and contradicts major global models where these systems are being helmed and restricted to central/state level public health governance authorities. This risk is only partially mitigated with the requirement that data can only be shared when it is "strictly necessary" to **directly formulate / implement** an appropriate health response. But as mentioned earlier, the Protocol's expansive definition of "appropriate health responses" fails to breed trust.

35. Para 6(b) states that response data in **de-identified form** may be shared with all the above, but also with *any ministries / departments* of the Government of India, or State / UT Governments, or Local Governments (as opposed to only Health Ministry / Departments). This allows for an unspecified number of agencies to have access to sensitive data which is contrary to law.

36. Further, the **de-identified** data can be shared where it is necessary **to assist in formulation / implementation** of a **critical health response**. The term "assist" amounts to a severely relaxed purpose limitation on the sharing of such data.

Further, the term **"**critical health response" is undefined in the Protocol which makes it even more vague than the broadly defined "appropriate health response".

Para 7: "Obligations on Entities with Whom Response Data is Shared"

37. Para 7(a) states that entities must only use response data "*strictly for the purpose for which it is shared*" and process it in a "*fair, transparent and non-discriminatory manner*". These entities cannot retain it "*beyond the period necessary to satisfy the purpose for which it is shared*" which is subject to the same 180 days time-limit. Further, entities "*shall also implement reasonable security practices and procedures*" as prescribed under any law in force [Para 7(a)]. Here,the Protocol fails to clarify if this is a reference to India's Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. This is because these Rules do not apply to Government but rather to private sector entities, and therefore breeds confusion rather than offering clarity. Moreover, the SPDI Rules are generally considered insufficient and already in the midst of being replaced by a new data protection law. Alternatively, if this is a reference to other data security norms, then they should have been explicitly referenced by the Protocol.

38. Para 7(b) of the Protocol also permits sharing response data with **third parties** "*if it is strictly necessary to directly formulate or implement appropriate health responses*". The entity sharing data is seemingly made responsible for ensuring adherence to the protocol by any other entity with which information is so shared.

39. Besides being subject to the same obligations under Para 7(a) of the Protocol, third Parties are also barred from re-use of data for other purposes or disclosing it to other entities. To ensure this, the Protocol states that third parties are subject to audit and review of their data usage by the Central Government [Para 7(b)].

40. **These Obligations cast by the Protocol are seriously deficient**. Para 7(a) uses the same vague, undefined, and loose terms that have been used elsewhere in the Protocol and the problems with the same need not be repeated here. The absence of any monitoring authority is a critical flaw which provides no oversight to minimise risk of excessive collection, sharing and improper use of data by government entities.

41. Further, it allows for sharing data with Third Parties where it is "strictly necessary" for the formulation of plans. It is not specified how this standard is distinct from the ideas of "assisting" or being "directly necessary" [Terms used in Para 6]. It is also not specified whether this applies to sharing only "de-identified" data or also extends to sharing "personal data".

42. **Finally, there is no reference for the need for individual specific consent or ability of individuals to revoke consent when it comes to third party access to data**

collected by the Aarogya Setu app. In fact, users of the Aarogya Setu app are not even afforded an avenue to audit the amount of data access, collected and processed by third parties. Citizens are not afforded any compensatory remedy under this provision should their data be abused or beached when controlled a third party.

Para 8: "Principles of Sharing of Response Data for Research Purposes"

43. The Protocol allows for **sharing response data for research purposes** with certain specified institutions / entities registered in India where the data has undergone "Hard Anonymisation". Hard Anonymisation has been defined as a privacy-securing process that is to be conducted as per protocols "*that are to be developed, reviewed and updated on a periodic basis by an expert committee appointed by the Principal Scientific Advisor to the Government of India*".

44. While the anonymisation of data as per protocols is laudable, it is important to note that nowhere does Para 8 require that these protocols be publicly shared, or be made available via an open access platform. Therefore, the public experts and external parties cannot study these anonymisation protocols, which means the public cannot empirically determine if technically robust means of "hard anonymisation" have been deployed.

45. Para 8 allows for the Government of India, is demonstration of the incentives for why the Government of India has taken a centralised approach. It is less about taking the least intrusive measure towards responding to the public health crisis, but more towards maximising the utility of data. In some ways it also shows an appetite on the Government of India to commercialise or discover commercial applications the Aarogya Setu app, rather than go the path of other democratic societies which are more focused on decentralised models which may effectively alert people to get tested and treated for the coronavirus itself. That such opportunities would be non-existent in a decentralised model of data storage only further supports the argument that the adoption of a centralised model for the Aarogya Setu App is not driven by purposes related to containing the spread of Covid-19. Additionally, it shows why the data retention limits of the Aarogya Setu programme do not apply to anonymised and aggregated datasets. Therefore, there is a greater need for public scrutiny on this front.

Paras 9 and 10: Violations and Sunset Clause

46. Para 9 of the Protocol states that any violations of the directions under the Protocol may lead to penalties under Sections 51 to 60 of the DMA "and other legal provisions". It is unclear whether such orders passed by an Empowered Group constituted under the DMA 2005 can also attract liability for non-compliance under the said statute.

47. The Sunset Clause (Para 10) requires a review of the Protocol after six months or at any earlier time as deemed fit, and also allows for the Empowered Group to extend the Protocol beyond the six month limit because of continuation of the Covid-19 pandemic in India. This renders it clear, therefore, that:

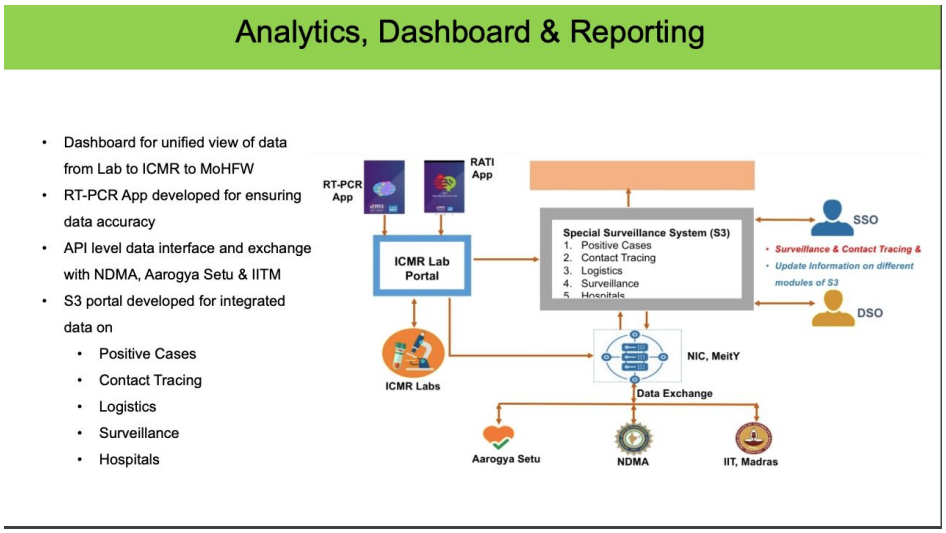
    A. **There is no sunset clause on the gathering of data by the Aarogya Setu Mobile Application**. In fact, the sunset clause potentially allows for gathering such data on even more relaxed terms and conditions.

    B. The Empowered Group can extend the Protocol on its own without any review by superior authorities which constituted the Empowered Group. Ideally such review should be administered through independent institutional mechanisms, disconnected from the executive.

    C. Finally, the Sunset Clause is insufficient since there is no reference to the actual destruction of servers and systems created as an output of the Aarogya Setu programme. Without such a reference, a sunset clause is meaningless and evokes concerns of the creation of a permanent infrastructure of Government surveillance.

Analysis of Press Release and Briefing Dated May 11, 2020

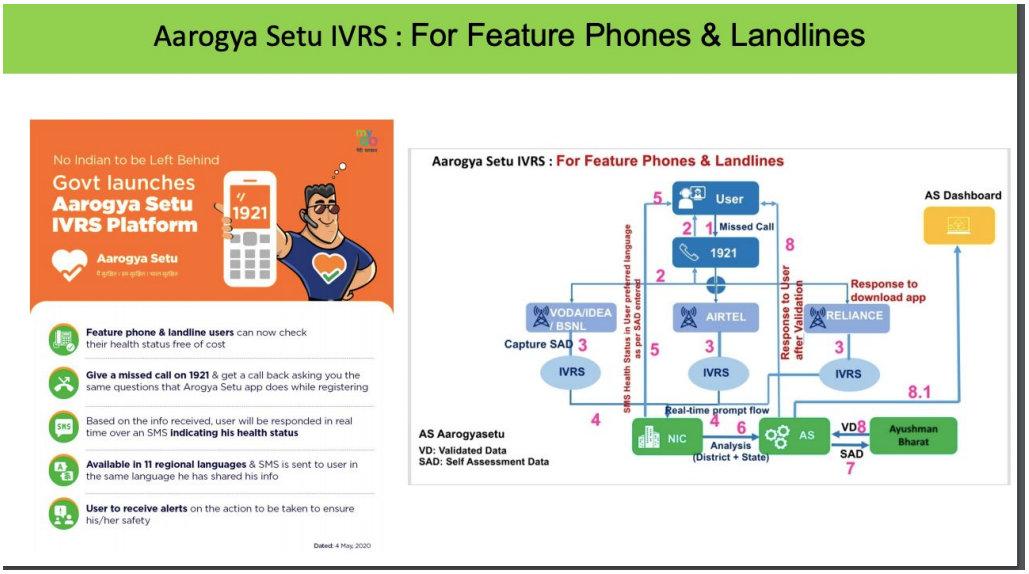
48. On the same day that the Government of India released the Protocol, MeitY Secretary, and the Chairperson of Empowered Group 9 Mr Ajay Prakash Sawhney did a press briefing on the Aarogya Setu app. The briefing was accompanied with a Press Release, via a powerpoint presentation. The PPT articulates the function of Empowered Group 9 on Technology and Data Management referenced above. The following captures a couple of troubling aspects we observed in the Press Release.



49. Slide 3 of the PPT clearly shows that the Government has set up a data exchange in which the Aarogya Setu database is being entangled with databases held by the National Disaster Management Authority, the Indian Council of Medical Research, and has already been granted access to a third party i.e. IIT Madras. We have two issues with this.

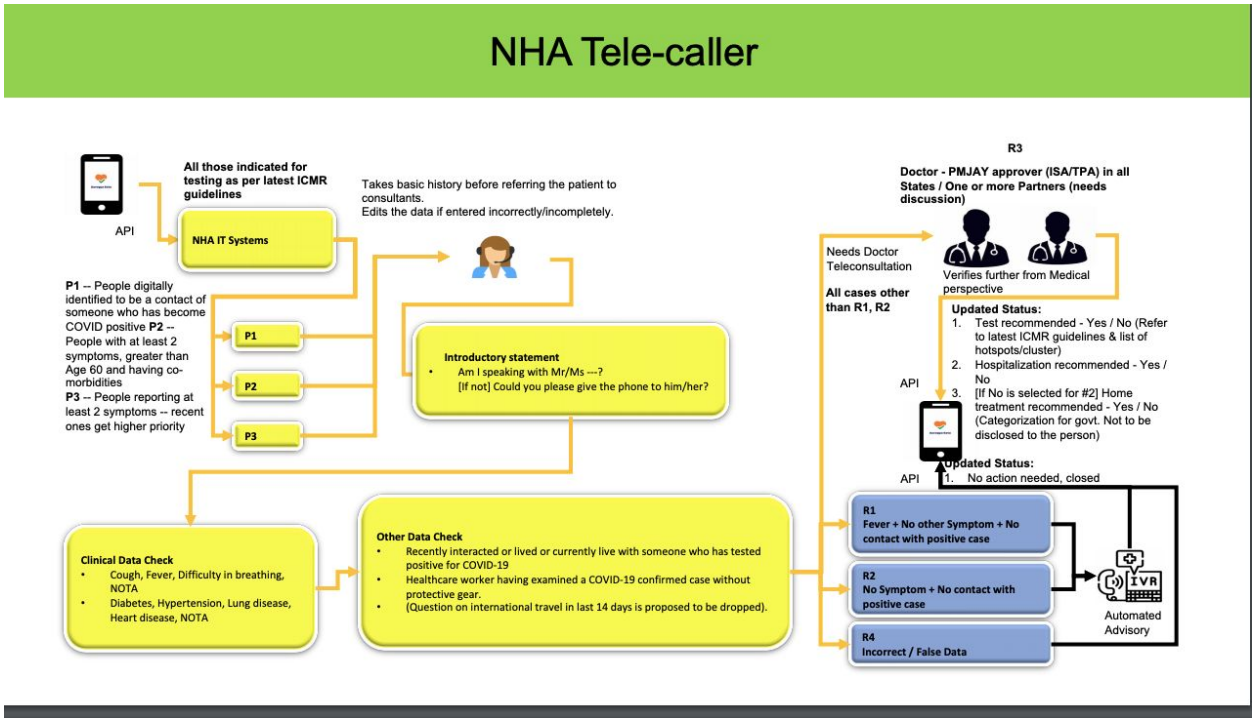
50. **First, this linkage of databases and sharing access to that data with a research institute is *prima facie* violating the latest Privacy Policy of the Aarogya Setu app. This is because while an earlier version of the Privacy Policy allowed for third party access to data collected, the latest version does not allow any third party access, until the Government of India issued the impugned Protocol. Therefore, the Government's data sharing practices have been breaching its own Privacy Policy for a meaningful period of time.**

51. Second, the above image confirms that the Government of India has already started linking/integrating the Aarogya Setu database with other Government and third party databases in a common server hosted by the National Informatics Centre. **Such linking of central databases makes it technically harder for complete destruction of databases**. Which is why international best practices have said that any central server should be isolated from other Government databases to ensure that all data generated and also inferences made by the app are completely destroyed. **There is a risk that without immediate intervention there is a risk of creating permanent government databases containing the personal and sensitive personal information of citizens which are being continuously analysed**.



52. Slide 15 of the PPT, discusses the IVRS platform. There is no discussion on how this system has been secured from manipulation or other attacks from malicious actors. The WHO refers to this aspect of the pandemic as an "infodemic" and it is a tool

through which one can spread panic within communities and could lead to unintended consequences wherein medical/testing centres are flooded, thereby stressing India's already scarce resources. As such these analog systems will collect very sensitive personal and personally identifiable information. There is a need for a disclosure on how privacy will be maintained in this context.



53. Slide 6 of the PPT discusses the backend of the Aarogya Setu and offers a clearer picture about how the Aarogya Setu app functions in the backend. It suggests that users will interface with human intermediaries including doctors as well. What the slide, the Protocol, the app's Privacy Policy and its Terms of Service fail to reveal is if someone may be determined to be Orange or Red **only** after human interaction, or if the algorithm may make decisions/assessments without the same. As the above slide does not sufficiently allay concerns of false positives. This is because in other contact tracing models, the exposure notification system is only activated after individuals have been tested at a medical facility and are confirmed to have been diagnosed with COVID-19.