Aarogya Setu

Why in news?

The Ministry of Electronics & Information Technology (MeitY) has issued a data-sharing and knowledge-sharing protocol for the Aarogya Setu app.

Why these guidelines are issued?

- The MeitY has laid down guidelines for sharing data with government agencies and third parties.
- Prior to this, the only legal shield around the mechanism was the app's privacy policy.
- The executive order issued came amid concerns expressed by a number of experts over the efficacy and safety of the app.
- The order says that in order to formulate appropriate health responses for addressing the Covid-19, data pertaining to individuals is required.
- These guidelines are issued to ensure that data collected from the app is gathered, processed and shared in an appropriate way.

What data can be collected and shared by Aarogya Setu?

- The data collected by the Aarogya Setu app is broadly divided into four categories which is collectively called response data.
- **Demographic data** includes information such as name, mobile number, age, gender, profession and travel history.
- **Contact data** is about any other individual that a given individual has come in close proximity with and the geographical location at which the contact occurred.
- **Self-assessment data** means the responses provided by that individual to the self-assessment test administered within the app.
- **Location data** comprises the geographical position of an individual in latitude and longitude.

What entities will be able to access this data?

- According to the protocol, the response data may be shared by the app's developer (National Informatics Centre) with the,
    1. Ministries and departments of Central/State/Union Territory/local governments,

2. National and State Disaster Management Authorities,
3. Public health institutions of the governments and
4. Other third parties

- The data can be shared only if it is strictly needed to directly formulate or implement appropriate health responses.
- For research purposes, the data can be shared with Indian universities or research institutions and research entities registered in India.
- The guidelines also empower universities and research entities to share the data with other such institutions.
- These entities can share only if such sharing is in furtherance of the same purpose for which it has sought approval to access such data.

What are the checks and balances?

- The protocol says the response data that can be shared has to be in **de-identified form**.
- Except for demographic data, the data must be stripped of information that may make it possible to identify the individual personally.
- These data must be assigned a randomly generated ID.
- To an extent, the NIC shall **document the sharing** of any data and maintain a list of the agencies with which data has been shared.
- The protocol also calls for any entity with which the data has been shared to not retain the data beyond **180 days** from the day it was collected.
- The protocol reads back to the Disaster Management Act, 2005 to establish the penalties in case of violation of the protocol.
- It also has a **sunset clause**, which calls for the empowered group to review the protocol after 6 months.
- Unless extended, the protocol will be in force only for 6 months from the date of issue.

How does the protocol disincentivise reversal of de-identification?

- Any entity which accesses anonymised response data shall not reverse anonymise such data or re-identify individuals in any manner.
- If any person takes any action which has the effect of such data no longer remaining anonymised,
    1. Any rights granted to them shall stand terminated, and
    2. They shall be liable for penalties under applicable laws for the time being in force.

What are the concerns?

- Legal experts have stressed the need for a personal data protection law to

back the government’s decision to make the app mandatory for everyone.

- The data being shared with third parties is a big concern.
- The third parties with which the data can be shared should have been listed to avoid possibility of misuse.
- The process of de-identifying the data should have been detailed, given that reversing de-identification was not difficult.

Source: The Indian Express