Aarogya Setu Data Access and Knowledge Sharing Protocol

Why in News

Recently, the **Ministry of Electronics and Information Technology (MeitY)** has issued **'Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020'** laying down guidelines for sharing such data with government agencies and third parties amid **Covid-19 pandemic**.

> The executive order issued came amid **concerns and privacy issues expressed by a number of experts** over the efficacy and safety of the app.

Aarogya Setu App

- It has been launched by the Ministry of Electronics and Information Technology.
- It will help people in identifying the risk of getting affected by the Coronavirus.
- It will also help to calculate risk based on the user's interaction with others, using cutting edge Bluetooth technology, algorithms and **artificial intelligence**.
  - Once installed in a smartphone, the app detects other nearby devices with Aarogya Setu installed.
- The app will help the Government take necessary timely steps for assessing risk of spread of Covid-19 infection and ensuring isolation where required.

Key Points

- **Description:**
  - The issued Protocol intends to ensure that data collected from the app is gathered, processed and shared in an **appropriate way.**
  - The **violation of the protocol** will lead to the penalties under the **Disaster Management Act, 2005.**
  - **MeitY** is designated as the agency **responsible for the implementation** of this Protocol. Further, the app's developer, **National Informatics Centre (NIC)** shall be responsible for collection, processing and managing response data collected by the Aarogya Setu app under this Protocol.
  - Further, it also calls for the **Empowered Group on Technology and Data Management** to review the protocol after six months; unless extended. It will be in **force only for six months** from the date of its issue.
    - **Empowered Group of Ministers** (EGoM) is a Group of Ministers (GoM) of the Union Government appointed by the Cabinet or the Prime Minister for investigating and reporting on such matters as may be specified.
    - These EGoMs are also authorised to take decisions in such matters after investigation.
- **Definition of Individual:**
  - The order states that the data pertaining to individuals is urgently required in order to formulate appropriate health responses for addressing the Covid-19 pandemic.
  - The Protocol clarifies that individuals means persons who are infected or are at high risk of being infected or who have come in contact with infected individuals.
- **Categorisation of Data:**
  - The data collected by the Aarogya Setu app is broadly divided into **four categories—**
    - **Demographic Data:** It includes information such as name, mobile number, age, gender, profession and travel history.
    - **Contact Data:** It is about any other individual that a given individual has come in close proximity with, including the duration of the contact, the proximate distance between the individuals and the geographical location at which the contact occurred.
    - **Self-assessment Data:** It includes the responses provided by that individual to the self-assessment test administered within the app.
    - **Location data:** It comprises the geographical position of an individual in latitude and longitude.
  - The demographic data, contact data, self-assessment data and location data are collectively called as **response data.**

- **Ground for Data Sharing:**
  - The data can be shared only if it is strictly necessary to directly formulate or implement an **appropriate health response.**
  - It can also be shared for **appropriate research work.**
- **Allowed Entities to Access Data:**
  - The **response data containing personal data** may be shared by the app's developer with the Health Ministry, Health Departments of State/Union Territory governments/local governments, National and State Disaster Management Authorities, other ministries and departments of the central and state governments, and other public health institutions of the central, state and local governments.
  - It can also be shared further with any **third parties** that include the Indian universities or research institutions and research entities registered in India.
    Further, the Protocol also empowers above mentioned universities and research entities to share the data with other such institutions.
- **Checks and Balances:**
  - **De-identified Form:** Except for demographic data, the response data must be stripped of information that may make it possible to identify the individual personally. **De-identification is the process used to prevent someone's personal identity from being revealed.**
    - Stripped information must be **assigned a randomly generated ID.**
    - The Protocol also discourages reversal of de-identification and imposes penalties under applicable laws for the time being in force.
  - **Maintenance of the List:** The NIC needs to maintain a list of, the agencies with the time at which data sharing was initiated, the categories of such data and the purpose of sharing the data.
  - **Data Retention:** Any entity with which the data has been shared shall not retain the data **beyond 180 days** from the day it was collected.
- **Concerns:**
  - There is a **need for a Personal data protection law** to back the government's decision to make the app mandatory for everyone.
    The **Personal Data Protection Bill 2019** is in the process of being approved by Parliament.
  - The **clause for data sharing with third parties is open ended** and has a highest possibility of being misused. The stated list of the third parties with which the data can be shared would have been helpful.
  - Further, the **process of de-identifying the data should have been detailed,** given that reversing de-identification was not difficult.

Source: IE