Health Data Management Policy - Privacy Concerns

What is the issue?

The CoWin portal for COVID-19 vaccines has come under criticism due to the absence of a privacy policy.

What is the Health Data Management Policy?

- CoWin follows the privacy policy of the National Digital Health Mission (NDHM) - the Health Data Management Policy.
- Other digital health initiatives, such as telemedicine, hospital management systems and insurance claims management, are also tied to this Policy.
- The Policy seeks to develop a national health information system.
- It facilitates the creation of Unique Health Identification (UHID) for individuals and healthcare providers.
- It also facilitates the collection, storage, processing and sharing of personal health information, as electronic health records (EHRs).
- Every individual's UHID is linked to his or her EHR.

What are the shortcomings?

- **Privacy** - Despite the benefits, digitisation entails significant risks to privacy, confidentiality and security of personal health data.
- The Policy aims to mitigate these risks, through two guiding principles:
    1. "security and privacy by design"
    2. individual autonomy over personal health data
- But fundamental 'design flaws' may end up increasing instances of personal health data breaches.
- **Legal backup** - The Supreme Court, in Puttaswamy case, held that the right to informational privacy is a fundamental right.
- Any encroachment on this must be supported by law.
- It also calls for enacting a comprehensive data protection legislation.
- Contrary to this, the digitisation process being rolled out under the NDHM Policy is not supported by any law.
- **Regulation** - Setting up a regulatory authority entails a law that defines the boundaries within which it can function.
- It should also ensure independence from government interference and accountability to Parliament.

- But the Policy itself establishes the NDHM to function like a regulator.
- It authorises the NDHM to perform legislative, executive and quasi-judicial functions and define its own governance structure.

What are the risks involved?

- There is a possibility of secondary use of digital health data for research and policy planning, particularly by private firms.
- The Policy permits sharing of aggregate and anonymised health data on the premise that anonymisation conceals individuals' identity.
- However, anonymised datasets can be easily de-anonymised to link back to personally identifiable information, risking individual privacy.
- The policy also does not stipulate 'data masking' as a measure available to individuals to ensure confidentiality of their data.
- [Data masking is a technique to hide specific sensitive health information in EHRs.
- Such information would be accessible even to health care providers only with the specific consent of the individual.]
- The Policy also does not limit the use of aggregate health data to public health purposes.
- Without strict purpose limitation, private firms may use people's health data to enhance profits.
- The Policy also does not require reporting of personal data breaches to affected individuals.
- This impedes the rights to information and access to grievance redress, as well as increases the possibility of illegitimate state surveillance.
- **Consent** - The guiding principle of individual autonomy is invoked through 'informed consent' for collecting and processing personal health data.
- The Policy mandates informed consent only prior to the collection of data.
- It applies in case of any change in the privacy policy or in relation to any new or unidentified purpose.
- This suggests that one-time consent for one or more broad purposes may be sufficient.
- But with this, individuals may ultimately end up with little or no control over their data.

What lies ahead?

- In a country with an uncertain cybersecurity environment, poor digital literacy and weak state capacity, the adverse implications of the above can be severe and widespread.
- Addressing the gaps in the Policy is necessary, but it is not sufficient.
- So, a comprehensive data protection law (with health sector specific rules) is

imperative for guiding the development of a digital health ecosystem.

Source: The Indian Express