The Big Picture: Health Data Management Policy

Why in News?

- The Health Ministry has approved the Health Data Management Policy under the **National Digital Health Mission (NDHM)** to protect and manage personal data of patients using the digital services of the scheme.
    - The policy was approved after a month of soliciting feedback from various stakeholders and the general public.

Key Points

- The policy acts as a guidance document across the **National Digital Health Ecosystem (NDHE).**
- The data collected across the National Digital Health Ecosystem (NDHE) will be stored at the central level, the state or Union Territory level and at the health facility level.
- The policy will be read along with and not in contradiction to, any applicable law or any instrument having the effect of any law together with the Blueprint, the information security policy, the data retention and archival policy and any other policy which may be issued for the implementation of the NDHM.

Salient Features of the Policy

- **Enabling document:** The policy is an enabling document before rolling out the National Digital Health Mission in its full fledged form.
    - The policy sets out the minimum standards for data privacy protection.
- **Doctors:** The authenticity of the doctors under this policy, will be taken care of by the **digidoctor platform** under which each and every doctor will be approved by the legitimate council.
- **A single platform:** The healthcare providers, under this policy will be connected by a single platform and they can still continue to hold the data after complying to certain standards that are prescribed.
- **Accessing the data:** The policy is just an initiative of connecting all the individual digital health systems with each other, to create an ecosystem to facilitate the access of data from one system to another.
    - The access to data is provided to ensure a quality healthcare.
- **Consent:** The doctor from any hospital can access a patient’s data but only if he/she gives the consent for the explicit information.
    - The healthcare providers shall be in a position to see the patient’s health status from any part of the country but only with the patient's consent.
    - It is also possible to give partial consent. The patient may provide the doctor the consent to view a certain health record and may restrict him from viewing other records.
- **The consent manager:** For consent, an electronic system called the consent manager will be introduced, every request for the data will be followed up by the consent manager which will verify

(a) identity of the person seeking data and (b) identity of the person who is providing the data.

    - It will also ensure that consent is provided and only after that the access to the data is provided.
- **Partial consent:** This type of consent will be required, if a person has to provide data only for a particular medical condition and his other medical records have nothing to do with the first one.

    - The person will be able to withdraw the consent from the record he does not want to show.
    - Also, the consent will only be provided for a particular period of time.

Digi-Doctor

- It is a comprehensive repository of all doctors practicing or teaching modern/ traditional systems of medicine. Enrolling on Digi-Doctor is completely voluntary and enables doctors to get connected to India's digital health ecosystem.
- Doctors from all systems of medicines (Modern Medicine – Doctors & Dentists, Ayurveda, Homeopathy, Unani, Siddha, and Sowa Rigpa), registered with their respective Medical Councils/ Registrars/ Boards can enroll on DigiDoctor.
- National Medical Council, Dental Council of India, Central Council for Indian Medicine, and Central Council for Homoeopathy are the National Councils overseeing enrollment along with the respective State Councils/ Registrars/ Boards.

Challenges

- **Lack of adequate laws:** Ideally, the policy should have been under the data protection law, but India currently has no data protection law.

    - The policy is intertwined with the **Personal Data Protection Bill.** It is still a debated topic in the parliament.
    - The laws we have right now are not adequate, the **Information Technology Act** is not particularly equipped for the challenges to be faced by this policy.
- **No laws for breachers:** The policy does not talk about what happens if a fiduciary breaches the data.

    - What will be the penalties charged if the privacy of a person is breached is not mentioned in the policy.
    - It is also not mentioned if the fiduciary who exploits the private information will still be a part of the network or not.
- **Electronic consent manager:** Ensuring there are no faults within the electronic consent manager is quite a challenge.

    - Also, the consent provided by a person is actually by his will cannot be assured through this method.

The Information Technology Act (IT Act), 2000

- It was enacted to give a fillip to electronic transactions, to provide legal recognition for e-commerce and e-transactions, to facilitate e-governance, to prevent computer-based crimes and ensure security practices and procedures.

The Personal Data Protection Bill

- The Personal Data Protection Bill was introduced in Parliament in 2019.
- The Bill seeks to provide for the protection of personal data of individuals (known as data principals), and creates a framework for processing such personal data by other entities (known as data fiduciaries).

- It provides the data principal with certain rights with respect to their data, such as seeking correction, completion or transfer of their data to other fiduciaries.
- Similarly, it sets out certain obligations, and other transparency and accountability measures to be undertaken by the data fiduciary, such as instituting grievance redressal mechanisms to address complaints of individuals.
- Processing of personal data is exempted from the provisions of the Bill in certain cases, such as security of state, public order, or for prevention, investigation, or prosecution of any offence.
- The Bill also establishes a Data Protection Authority to ensure compliance with the provisions of the Bill and provide for further regulations.

Way Forward

- **Blockchain technology:** Improvising blockchain into the NDHM will be a concrete step towards protection of sensitive health data privacy.
- **Need for a data protection law:** To make sure that data which is given to different fiduciaries and being shared across different entities is safe and protected, a stringent law needs to be formed.
- **Ensuring confidentiality:** Data security and privacy of patients being one of the biggest concerns makes it a mandate to ensure that the health records of the patients remain entirely confidential and secure.
    - Who's actually accessing the data needs to be checked upon.
    - Introducing an anonymisation protocol within the platform can help ensure the privacy of the patients.

Conclusion

- While the government is trying to digitize the medical sector, the Digital Health Management Policy is a milestone in the medical field which can make possible the better management of data of individuals to help them get better medical facilities.
    - Moreover, telemedicine is a pioneer of digital treatment of patients and it is cost effective too.
- However, concerns related to security of data of patients and the lack of any rock solid data protection act stand as a big challenge and should be the key area of focus.