Biological Data Storage, Access and Sharing Policy in India

July 26, 2019
<u>Source:</u> *The Hindu*

Manifest pedagogy

Data and news around it are are of high importance. When it is biological data, the topic becomes even more important. Many debates around biological data are going on among which this topic is highly relevant to UPSC. Also one has to study this topic from the angle of ethics as well

In news

- The Department of Biotechnology (DBT) has invited comments on 'Biological Data Storage, Access and Sharing Policy of India' from all the stakeholders engaged in research & development in Biological Sciences

Placing it in syllabus

- S and T developments and their applications

Current dimensions

- What is the policy about?
- Framework for data sharing in the policy
- Necessity of the policy
- How Ethical concerns are addressed

Content

To define guidelines for sharing of data generated by scientists in India using modern biotechnological tools and methods, DBT has issued the 'Biological data storage, access

and sharing policy of India'.

Necessity of the policy:

Advances in DNA sequencing and other high-throughput technologies have enabled government agencies to fund research towards generation of large volumes of biological data in various sectors of Biosciences. Several scientists use government funds to conduct research and collect biological specimens and data such as DNA samples, cell and tissue samples, store these details in databases and often lock them up barring access to other researchers and scientists who may be interested in them.

This leads to duplication of data collection exercises, lost opportunities to access data collected over the years and a wastage of public money. Therefore, DBT prepared Zero Draft on 'Biological Data Storage, Access and Sharing Policy of India (BDSASP)' aiming at broad research use of biological data that enhances public benefits by facilitating speedy discoveries in biosciences directly associated with human being.

According to the draft, "Raw (Level-1) data must be shared, by placement on a database identified and approved by the funding agency of the Government of India, within one year of generation of the data. If no such database is identified by the agency, then raw data must be made available to anyone working in any Indian institution, public or private, requesting for these data".

Data generated from public funds are for public good. The necessity of data-sharing is to accrue maximal benefit from public investment in generation of data

What is the policy about?

This document provides broad guidelines for biological data in general and pertains to modern high-throughput, high-volume data in particular. (e.g. data generated by nucleic acid

sequencing and microarrays, biomolecular structures and flow cytometry). The guidelines allow for easily sharing the data not just with public research facilities, but also private labs and even for international collaborations. The guidelines aim to create a central National Biological Data Bank

Framework for Data Sharing and Access

(a) Data generated from publicly-funded projects should be shared openly for public good, safeguarding the ethical issues that may arise out of shared data.

(b) High standards and best practices should be used in generation, management and access to data.

(c) Shared data will always be de-identified.

(d) Under specific circumstances, even data generated using public funds may not be provided open access, and may be provided under a managed/controlled access protocol.

(e) To enhance use of data, metadata must also be released in a timely manner.

(f) Access to data that are of "sensitive" nature may be barred, even if generated using public funds.

(g) The conduct of research must not be jeopardized by release of data. The research organization must ensure that due consideration is given to protect the interest of the data generator.

(h) There may be a period of moratorium before the data generator releases the data in the public domain. The period of moratorium may vary with the nature of the data; public resource data need to be released without any significant time lag

Addressing ethical concerns:

Since data are a public resource, there are primarily three stakeholders: resource funders who help generate this resource, producers and users of this resource. All three stakeholders must assume responsibility on how the data may be shared. Even though data are a public resource, sharing of data have ethical implications

- Responsible data-sharing implies that certain **principles** are to be followed. These include, **Protection of privacy and confidentiality:** Shared data must not include any personal identifiers and must have been collected with informed consent, including consent to share data after adequate de-identification.
- Care must be taken to ensure that the data resource is not used to ostracize communities; ethnic, religious, geographical or any other.
- Appropriate ethical approval(s) need to be obtained by the data-submitter prior to data submission.
- The quality of the data must be of a high standard, unbiased and verifiable. The data submitter is responsible for ensuring high quality and authenticity of submitted data.
- Appropriate security features must be embedded in the storage and access framework to avoid breach of data-trust.
- Features to enable tracing of chain of data access may be built-in.
- Mechanisms for obtaining feedback from resource users must be put in place in order to improve data quality, data access, data integrity and interoperability.
- Data-sharing policy must be transparent and must state in a publicly-accessible manner the policy of data transfer within and across national boundaries, with public and private organizations, for knowledge and commercial use, etc.
- There should also be a formal mechanism to register complaints of data misuse and to handle such complaints.

There are many issues that must be taken into account in the context of datasharing. Data may induce vulnerability to individuals and to populations. The rights to privacy and confidentiality of individuals and populations must be protected as emphasized in the UN Declaration of Human Rights and no harm must be done to them as a result of data-sharing