All India Institute of Medical Sciences, Jodhpur

Data Sharing Policy

Contents:

Data Sharing Policy (Final_08.06.2024)

1. BACKGROUND

1.1 About Data Sharing

All India Institute of Medical Sciences, Jodhpur encourages research with good clinical practice and high ethical and scientific standards. AIIMS Jodhpur provides a research ecosystem which is collaborative, transparent and evidence based. For fostering collaborations, the sharing of data with other research organizations is a need of the hour. So, in order to achieve scientific progress and advancement of knowledge, institute has formulated a policy of data sharing, along with the processes to be adopted in order to ensure responsible sharing of the data.

1.2 Scope

This data sharing policy will cover type of data, mode of sharing of data, boundaries of data inclusion, of all the studies conducted in India or in collaboration with national and international agencies, regardless of the source of funds.

The policy will address following areas (not limited to):

1. Categories of data to be shared
2. Data formats and domains covered (clinical trial, genomic, survey responses, etc.)
3. Specific types of proposals or data generated from all research conducted in the institution and ensure that there is accuracy and transparency about the research and the data while maintaining the privacy and autonomy of the participants (patients)

2 RESEARCH DATA AND KEY CONCEPTS

2.1 Key Concepts in Understanding Data Sharing Considerations

As healthcare entities, including the government, strive to deliver optimal care, it is the patient's needs that drive the services offered. From the moment a patient enters a healthcare facility to their exit, their journey is marked by numerous steps, generating significant amounts of data along the way.

A patient undergoing a surgical procedure begins with an outpatient visit, followed by diagnostic tests, treatment, and possibly surgery. Throughout this process, sensitive information is shared and stored in healthcare systems, shaping the patient's experience and outcomes. Furthermore, patients may be explained and requested to provide consent for various research procedures associated with the entire

proceedings.

Given the intimate nature of this data, it is essential for healthcare providers to prioritize both patient care and data privacy. By implementing appropriate measures, providers can ensure not only improved healthcare outcomes but also safeguard patient confidentiality. This approach fosters a resilient and adaptable healthcare ecosystem, dedicated to delivering effective care to every patient, while maintaining data privacy and stringent anonymity. In this context, it is important to define few key terminologies in order to develop a holistic understanding about data privacy and data sharing norms:

2.2 Personal Health Data

All data gathered during the provision of healthcare services falls under the umbrella term of Personal Health Data. This encompasses several key categories:

Demographic data includes details like age, gender, race, marital status, address, emergency contacts, and information about immediate family members. Additionally, it may entail details regarding employment, education, and indicators of socioeconomic status.

Administrative data covers information related to health insurance, such as eligibility, coverage details, and co-payment requirements. It also encompasses data on services provided, including charges and insurance settlements, along with identifiers for healthcare providers and specific details about their practice.

Health risks information pertains to behaviors and lifestyle factors, family medical history, and genetic predispositions to certain conditions.

Health status reflects individuals' self-reported physical, mental, emotional, and social well-being, as well as perceptions of their health relative to peers.

As databases become more comprehensive, they may contain increasingly recent and sensitive information about individuals. Consequently, the depth of information collected raises concerns regarding privacy and confidentiality.

2.3 Data Collection

Data Collection involves the gathering, acquiring, or obtaining of personal information to be included in a record or publication. In the healthcare context, this typically involves obtaining health information directly from the patient or from other sources and storing it in a database.

Examples of data collection methods include:

- Recording patients' statements or your own observations about what a patient has communicated.
- Requesting patients to complete forms with details such as name, address, date of birth, and medical history.
- Incorporating specialist reports provided by patients into their medical records.
- Collecting physical or biological samples from patients and labeling them with their name or other identifying information.
- Storing video footage, photographs, or audio recordings in which a patient can be reasonably identified.
- Retaining emails or other correspondence containing personal information about a patient.
- From the electronic Hospital Data system

2.4 Consent

Consent refers to the explicit approval, only in writing, through a clear and affirmative action. In certain healthcare emergency situations, where immediate action is necessary, personal data may be used without explicit consent, relying on the circumstances and the patient's conduct for validity.

In this guide, consent pertains to patients' decisions regarding how organizations handle their health information, distinct from consent for receiving treatment. While often given simultaneously, they represent distinct actions by the patient towards different aspects of their care.

Key elements of consent include:

- Being adequately informed before giving consent.
- Giving consent voluntarily, without coercion.
- Obtaining consent from individuals who have the capacity to understand and communicate their consent.
- Ensuring consent is current and specific to the intended use.
- Patient has the right to withdraw the consent and opt out anytime

2.5 De-Identification and Anonymization

De-identification:

Personal data is considered de-identified when it no longer pertains to an 'identifiable individual'. Despite being de-identified, such data is still classified as 'personal data'. Typically, de-identification involves two main steps:

- Removing personal identifiers like name, address, or date of birth, which could lead to identification.

- Eliminating or altering other details that could potentially allow identification, such as unique characteristics or combinations of characteristics.

However, it is important to note that de-identification may not completely eliminate the risk of re-identification. There is a possibility that additional data or information could be matched with the de-identified data. Therefore, assessing and mitigating the risk of re-identification is crucial. Factors to consider in determining the effectiveness of de-identification may include cost, difficulty, practicality, and the likelihood of re-identification.

Anonymization:

Anonymization occurs when both direct and indirect identifiers are removed or manipulated, accompanied by mathematical and technical measures to prevent re-identification. Anonymization should aim to prevent:

- Singling out: This involves isolating records that could potentially identify an individual within the dataset.
- Linkability: Referring to the potential isolation of records that could identify an individual.
- Inferences: This refers to the ability to deduce the value of an attribute based on other attributes with significant probability.

The anonymization process must be irreversible and adhere to methods and techniques accepted by the relevant regulator.

2.6 Disclosure

Disclosure of health information occurs when it is made accessible to parties outside the primary organization, and subsequent handling of that information falls beyond the effective control of the organization that originally gathered or held the data. This encompasses scenarios such as sharing health information with related corporate bodies.

Examples of disclosure include:

- Sharing health information with another healthcare provider or individual.
- Accidentally providing health information to an unintended recipient.
- Inadvertently displaying a computer screen containing health information where it can be viewed by others, such as at a reception counter or in an office.

2.7 Processing:

Processing of health information involves handling, managing, or utilizing it for activities within an

organization's effective control. Examples of processing include:

- Accessing and reviewing a patient's medical file.
- Searching electronic records for a patient's health information.
- Making treatment decisions based on a patient's health data.
- Sharing the information with other departments within the organization.

Processing encompasses all operations performed on personal data throughout its lifecycle within an organization's effective control. ***(DSCI Sectoral Privacy Guide | Healthcare, 2021)***

3 DATA SHARING POLICY AND DATA SHARING AGREEMENT

3.1 Data Sharing Committee (DSC) at AIIMS Jodhpur

A Data Sharing Committee (DSC) will be responsible for the enforcement of the developed policy and providing guidance in the related procedures regarding the data sharing protocol. The committee will monitor the Data Sharing Plan (DSP) and Data Sharing Agreement (DSA) of research proposals submitted to the Executive Director for necessary approvals. The committee will ensure that the data sharing in any project is in accordance with the submitted DSP and DSA. The decision of the committee shall be considered final when the request of sharing of data is received. In case of any grievance, the Executive Director, AIIMS Jodhpur will be the appellate authority.

3.2 Role of Principal Investigators, Data Sharing Plan and Data Sharing Agreement

The investigators at the institute will hold the responsibility to:

1. Generate complete and quality data from the research project.
2. Provide necessary information in a prescribed institutional format of DSP and DSA *[Annexure A]*. Any vital information considering terms and conditions laid in grants and contracts of the funding agencies, as well specific local and regional requirements should be made available as an annexure with the DSP/DSA formats.
3. If there is a DSP during the initial conceptualization of the research projects, the same should be mentioned in the very beginning. The DSP and DSA can be submitted along with the research proposal during the initial submission. In case, such a request by any agency is received later, the received request along with the DSA / DSP should be sent to the Executive Director for necessary approvals.
4. Abide by the International Committee of Medical Journal Editors' (ICMJE) requirements.

4 DATA SHARING, DATA GENERATION AND PUBLICATION

4.1 Data Sharing: The DSP should mention with full clarity about mutual agreement on access and extent of access of available relevant information owned by the Principal Investigator. There should be

a clear mention of agreement to use, share, maintain, access, and/or control such information in accordance with applicable law, including all relevant laws pertaining to the use of personal data and non-personal data.

4.2 Necessary Clauses in the DSP and DSA:

1. **Data Utilization:** DSP and DSA should clearly mention that the data will be shared exclusively for health and medical research purposes, adhering to the consent parameters established during the initial data collection.
2. **Proposal Restrictions:** Request for data sharing proposals that could reveal or risk revealing the identities of participants in active or ongoing randomized trials will be rejected.
3. **Eligibility to Request:** Only individuals affiliated with recognized academic, healthcare, or pharmaceutical organizations, and who possess medical research experience, are eligible to request data.
4. **Conflict of Interest**: Requesters are obligated to disclose any real or potential conflicts of interest that might affect their analysis interpretation. This includes declaring all funding sources for the intended research with the requested data set, both current and future, to the Institute. Such disclosures must also be made in any resultant publications or presentations. The Institute retains the discretion to deny data access if there is a possibility of adversarial conflicts of interest.

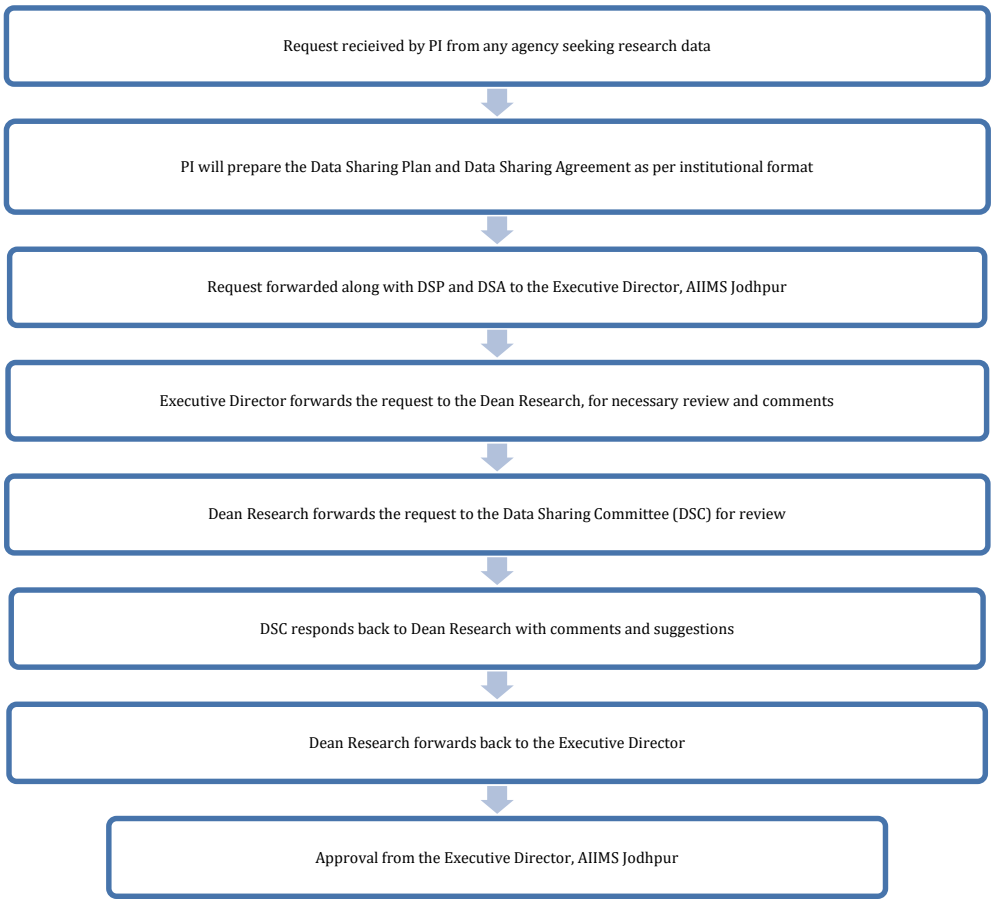
4.3 Data Sharing Procedure

- **Initial Contact**: Interested organisations/individuals are expected to first informally consult with the study's principal investigators to assess the viability of data sharing.
- Any data sharing will be approved/accepted as the collaborative research project involving the institute.
- **Study Proposal Submission**: A detailed proposal with data sharing plan to be developed by the PI who has received the request. This document should clearly articulate the research background, objectives, proposed methodology, and include pertinent references. The received request along with the DSP should be forward to the Executive Director.
- **Proposal Evaluation and Approval**: The DSC will evaluate the submitted proposal. The DSC will ensure that the PI is the actual custodian of the requested data. All approvals are subject to the Data Sharing Committee's oversight.
- **Appeal Procedure**: In case the DSC disapproves or declines the request of data sharing, the requesters have the right to appeal against the decision to Executive Director, AIIMS Jodhpur.
- **Ethical Clearance**: It is the requester's obligation to secure approval from their own ethics committee, and potentially from the Research Ethics Committee overseeing the Institute's study.
- **Cost Responsibility:** Requesters are responsible for all costs associated with data sharing

administration, which may include legal fees, as well as the retrieval, processing, and delivery of data. Cost estimates will be provided following the preliminary application assessment.

- **Access Conditions:** No data should be made accessible to any individual without having a formal application routed through the DSC.

Data Sharing Procedure



4.4 Terms of Sharing:

- **Agreement Compliance**: The requester shall engage in a Data Sharing Agreement that aligns with the Institute's stipulations.
- **Transfer Limitations**: Data dissemination is restricted solely to the individuals specified in the initial request.
- **Internal Use**: Data transfer beyond the requester's research team is prohibited.
- **Purpose Specification**: Usage of the provided data is confined to the objectives outlined in the Proposal and the Data Sharing Agreement.
- **Anonymity Assurance**: All distributed data will be anonymized, with no identifiable information

accessible to the requester. De-identification procedures will follow the guidelines set by the relevant study Custodian or Data Sharing Committee.

- **Identification Prohibition**: The requester and their team are forbidden from attempting to identify individuals from the data. Inadvertent identification must not be documented or disclosed and should be immediately reported to the Institute.
- **Linkage Restriction**: Recipients must not merge the anonymized data with other datasets without explicit authorization from the Custodian or Data Sharing Committee.

4.5 Ownership and Rights

i. **Data Generation**: Any and all data/information generated through the Research Collaboration shall be jointly owned by AIIMS Jodhpur and the requesting individual/organization as per clearly mentioned statements in the DSA.

ii. **Publication**: The publications will be jointly authored.

iii. **Dispute Resolution:** For any type of dispute, the resolution will be done by mutual understanding and in case of appeal, the decision of the Director, AIIMS Jodhpur will be considered final.

iv. **Intellectual Property Rights:** The IPR will be as per the IPR Policy of AIIMS Jodhpur.

Annexure A – Data Sharing Plan Template

DATA SHARING PLAN
All India Institute of Medical Sciences, Jodhpur

1. **Principal Investigator Details**
   Name:
   Designation:
   Department:

2. **Project Details**
   Type of Project: ***(Intramural/ Extramural/ Non-funded)***
   Name of Funding Agency:

3. **Data Type** ***(Select checkbox, whichever apply)***
   - **A.** Data involves rDNA technology ☐
   - **B.** Data involves Micro-organisms ☐
   - **C.** Data involves Animal Studies ☐
   - **D.** Data involves Biomedical and Health Research involving Human Participants ☐
   - **E.** Data involves Import/Export/Transfer (MTA needed) ☐
   - **F.** Data involves Radioactive Material ☐
   - **G.** Data confined to field trials for Genetically-Engineered Products ☐

4. **Related Tools, Software and/or Code**
   State whether specialized tools, software, and/or code are needed to access or manipulate shared scientific data, and if so, provide the name(s) of the needed tool(s) and software and specify how they can be accessed.
   Yes ☐ **No** ☐ **Not Applicable** ☐
   If Yes, please describe:

5. **Data Preservation, Access, and Associated Timelines**
   A. **Repository/Server where scientific data will be archived:**
   Provide the name of the repository(ies) where scientific data and metadata arising from the project will be archived.
   Yes ☐ **No** ☐ **Not Applicable** ☐
   If Yes, please describe:

   B. When and how long the scientific data will be made available:
   Describe when the scientific data will be made available to other users and for how long data will be available.

6. **Access, Distribution, or Reuse Considerations**
   Protections for privacy, rights, and confidentiality of human research participants:
   Please mention how the data will be de-identified and anonymized and any other protective measures, wherever necessary

Ref.: Data Management and Sharing. NIH (grants.nih.gov)