MAINTENANCE OF RESEARCH

DATA AND RECORDS

Indian Institute of Technology Patna

Introduction

Research data created while individuals are pursuing research studies as faculty, staff or students at IIT Patna and data created by visiting scientists utilizing the facilities of the institute are owned and retained by the institute. The creation and maintenance of records is integral to the research process. Complete, authentic and reliable records are required to:

- demonstrate good research practice and strengthen the reliability of research evidence;
- safeguard researchers and institution from allegations of research misconduct;
- demonstrate effective stewardship of resources to auditors and to research sponsors;
- protect individual and institutional intellectual property rights;
- demonstrate compliance with legislation, regulations and other requirements.

What are research data?

Research data are documents or other items which contain recorded information; produced or received in the initiation, conduct or completion of an activity and retained as evidence of that activity, or because they have other informational value. It include laboratory notebooks, as well as any other records that are commonly accepted in the research community as necessary for the reconstruction, evaluation and validation of reported results of research and the events and processes leading to those results, regardless of the form or the media on which they may be recorded. The recorded information may be in any form (e.g. text, image, sound) and the records may be in any medium or format, including three-dimensional objects.

Research records associated with the research process can be organized into four categories:

1. Records documenting the research process e.g. research protocols; applications for regulatory approvals and approvals granted.
2. Records documenting research outcomes or products e.g. technical reports; monographs.
3. Records documenting the management of the research process/project(s) e.g. applications for funding; contracts; purchase invoices; staff timesheets.
4. Research data in both ‘raw’ and ‘analyzed’ form e.g. notes; completed questionnaires; audio/video recordings; photographs; instrument readings; databases; samples.

The specific types of records in each category vary, depending on the research discipline and the characteristics of projects but some types are common to most research activities (e.g. correspondence (including e-mail), laboratory notebooks).

Who is responsible for managing research records?

The Principal Investigator/ Supervisor is, by default, responsible for the accuracy, completeness and security of all the records produced during a research project. If the Principal Investigator/ Supervisor delegates any responsibilities for managing records to other members of a project team, she/he should define and document these arrangements, and make sure that the other members of the team are aware of them.

A Principal Investigator/ Supervisor has the responsibility of advising the students on the nature of data to be collected, the methods to be applied, and on the nature of research outcomes, clearly specifying the procedure to be followed for recording the research data and retaining them, overseeing the recorded data and signing the records periodically, retaining the submitted data, records, and notebooks carefully for future use, leaving the research data and records in the custody of the Head of the Department if he (or she) leaves the Institute for good.

In case of sponsored project the Principal Investigator will handle all responsibilities of managing records after a project has been accepted. A copy of intermediate and final reports sent to the sponsoring agency will be kept with R&D documents of the project file.

The Head of an academic unit (Department/Center/School) has the responsibility of issuing blank laboratory notebooks to the student through the supervisor after duly recording the same, arranging to retain the submitted research data and files with proper indexing, retaining them for at least five years (and if needed for more number of years) and authorizing their destruction after that, and reporting compliance in record bookkeeping at specified times.

Where and how should research records be stored?

1. Research records should be stored in facilities and equipment (‘hard copy’ records) or in electronic systems (digital records) which are ‘fit for purpose’.

   ‘Fit for purpose’ means:
   - **adequate space** for all the records which need to be produced and retained;
   - **appropriate security measures** to control access to the records;
   - **appropriate environmental conditions** for the record media used.

2. Storage facilities and systems should meet the same standards irrespective of where they are located and who is responsible for managing them.

3. Designated staff should maintain a record of:
   - the content, format and location of all research records;
   - research records which have been transferred to another organization (e.g. returned to a sponsor, deposited in a third-party data archive);
   - research records which have been made available (directly by the institution) for reuse/ re-purposing by third parties;
   - the destruction of research records, including the authority for destruction and the date of destruction.

4. During a research project, research records should be stored and indexed so that they can be identified and retrieved quickly and easily.

5. Paper documents and other ‘hard-copy’ records should be housed in durable containers which are clearly labeled with key information needed to identify them, and these containers should be stored in secure facilities and equipment.

6. Confidential ‘hard-copy’ records should be stored in locked equipment or rooms when they are not being used.

7. Electronic records should be organized in accordance with institutional protocols for titling, classification and indexing.

8. Confidential electronic records should be protected with passwords and other electronic security measures.

9. If electronic systems are not centrally managed, designated staff should make back-up copies to prevent loss of records through accidental or intentional damage or destruction.

10. When research records become (relatively) inactive after the completion of a project, they may be transferred to other storage facilities or systems. However, it must still be possible to identify and retrieve them easily and within an acceptable time.

How long should research records be kept?

Some research sponsors specify requirements for retention of specific categories of records. Research is a complex activity and every project is unique. Applying the institution’s records retention policy to the records of an individual research project involves assessing:

- the risks of not having access to evidence of decisions made, actions taken and results produced during the project;
- the benefits of retaining records containing this evidence, for the institution, for the wider academic community and for society as a whole;
- the costs of retaining these records, including the costs of facilities and equipment to store them and of staff to maintain them and provide access to them.

Specific issues to consider in determining retention periods for records of a research project include:

- whether records should be retained to support a patent or other protected intellectual property;
- whether the research has been linked to inquiries or investigations, such as allegations of scientific or financial misconduct;
- whether the research has been controversial or ground-breaking.

Where the nature of the records makes it impossible, or prohibitively expensive, to preserve them for the required or selected retention period (e.g. biological samples), the Principal

Investigator should consider what other means are available to preserve the evidence they contain.

Notebooks and electronic records

The following basic policies apply:

- All raw data should be recorded and retained in indexed laboratory notebooks with permanent binding and numbered pages or in an electronic notebook dedicated to that purpose. The guidelines of laboratory notebook should be followed strictly.
- Machine print-outs, questionnaires, chart recordings, autoradiograph, etc which cannot be attached to the main record should be retained in a separate ring binder/ folder that is cross-indexed with the main record.
- Records in notebooks should be entered as soon as possible after the data are collected. Recorded data should be identified by date of the record and date of collection if the two do not coincide. Subsequent modifications or additions to records should also be clearly identified and dated.
- Special attention should be paid to recording accurately the use of potentially hazardous substances (e.g., radioactive materials) in both laboratory notebooks and any central logbooks.
- In clinical studies, consent forms should be kept securely with the raw data, and normally for the same period of time.
- Supervisors should regularly (monthly or as appropriate to the nature of the work) review and "sign-off" notebooks of researchers to signify that records are complete and accurate. Queries should be discussed immediately with the individual who recorded the data and any resultant changes to the records should be signed by both. Authentication of data collected and recorded electronically requires special consideration.

Computer-generated data

Special procedures are necessary for electronically generated data.

- Data should be backed-up regularly; duplicate copies should be held on disc in a secure but readily accessible archive.
- Where feasible, a hard copy should be made of particularly important data.
- Copies of relevant software, particularly the version used to process electronic data, must be retained along with the raw data to ensure future access. Software updates must be logged and stored as new formats and media are adopted.
- Special attention should be paid to guaranteeing the security of electronic data.

Access to research records

Access to research records should be controlled to prevent unauthorized use, removal or destruction of the records themselves and unauthorized disclosure of information they contain.