Guidance for Research Data and Materials Security

This is a practical supplement to the Guidance for Ethical Use of Data in Research. These technical and administration best practices should be carefully considered during the design of research involving human subjects. Review of protections for research data is a critical component of the IRB review process.

The best practices described in this guidance are consistent with National Institutes of Health (NIH) and National Research Council (NRC) guidelines.[1] These policies are also compliant with HIPAA, even though LU is not considered a "covered entity." For studies involving substances, agents, or devices, these polices reflect Food & Drug Administration (FDA) and MO Bureau of Narcotics and Dangerous Drugs (BNDD) regulations, though additional policies apply for use of controlled substances. Additional policy and regulation may apply depending on funding, location, and research design. Investigators at Lindenwood University are responsible for compliance with all applicable data or materials security requirements.

The Lindenwood University IRB is available for consultation on compliance with data and materials security or sharing requirements. The IRB consults with Lindenwood University IT staff to affirm technological validity of proposed security protocols.

1. What Technical Safeguards should be considered for research data?

- Access to research data collection and storage devices must be limited to members of the research team, who are listed on the approved LU IRB application.
- All data collection and storage devices, such as portable drives, must be password protected with a strong password compliant with LU IT standards.
- Phones and devices with an automatic connection to cloud storage may not be used to record images of sensitive information. A digital camera or device disconnected from the internet should be used to capture images, which should then be transferred to a secure server as soon as possible and deleted from the device.
- Audio records collected for research purposes should be transferred to a secure server as soon as possible and deleted from the device.
- Any code or key used to link participant identifiers and research participant data, surveys, or case report forms must be stored in a location separate from the research data. For example, research data could be kept in one password protected folder and the linked code could be kept in a separate password protected folder.
- Duplicate records should be kept of all electronic records. The investigator should maintain a log of all locations of research records, to facilitate backup and restoration of data.

[1] NIH "Guidelines for Scientific Record Keeping" https://oir.nih.gov/sites/default/files/uploads/sourcebook/documents/ethical_conduct/guidelines-scientific_recordkeeping.pdf; NRC "Prudent Practices in the Laboratory": https://www.nap.edu/catalog/12654/prudent-practices-in-the-laboratory-handling-and-management-of-chemical

- Research data involving sensitive information should not be stored on personal computing devices or in a home office setting. Primary data storage should take place on Lindenwood University servers or another setting approved by the IRB.
- All electronic records of human research data collection may only be deleted after compliance with the LU research record retention policy (three years) has been met.

2. What Physical Safeguards should be considered for research data?

- Basic security measures for laboratories supporting research involving human subjects must be maintained. Basic measures include physical key, code, or card access, a log of individuals currently approved to access the space, sign-in procedures for guests or research participants.
- Hard copies of research records must be stored in a secure location with reasonably controlled access. For example, a locked cabinet in a locked faculty office would be appropriate. A locked cabinet in a lab, classroom, or similar high traffic area would not be appropriate. The following are considered hard copy research records:
    - Laboratory notebooks, when they contain data collected during research involving human subjects.
    - Signed Consent Documents.
    - Completed surveys, case report forms, or any hard copy form or instrument used to capture data during research involving human subjects.
    - Documentation of IRB approval and communication, and any other related regulatory documentation.
    - Any notes to file or related documentation created during the conduct of research involving human subjects.

- Hard copies of research records involving health information must be stored in a secure location with controlled access, and may be subject to additional controls or agreements as determined by the IRB. Health information is defined as “any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.”
- All hard copy records containing health information must be stored behind two physical locks (e.g. a locked office door and locked file cabinet).
- Any code or key used to link participant identifiers and research participant data, surveys, or case report forms must be kept in a location separate physical location from the research data.
- All paper records of human research data collection may only be destroyed after compliance with the LU research record retention policy (three years) has been met.

3. What practices should be considered for moving, transferring, or sharing research data?

- If any hard copy research records are physically moved, care must be taken to ensure hard copies are enclosed and remain confidential at all times.

- Any file transfer protocol for the transmission of human subjects research data from one party to another (e.g. email, cloud file sharing, large file transfer, etc…) must be approved by the IRB prior to use. Additional consultation with LU IT to ensure security may be required.
- Flash drives or portable devices must be encrypted if they are used to store or transfer human subjects research data. Data must be uploaded to a password protected PC or server as soon as possible, and all data must then be deleted from the drive or portable device.
- There are many cases in which data are collected in the field and then must be transferred to a personal computing device or a cloud storage platform. This type of interim data storage is acceptable provided it has been approved by the IRB.
- Data involving health information may not be shared by email excepting within the LU Outlook email environment.

4. What practices should be considered for research materials or human tissue?

- Laboratory Materials and Equipment:
    - Lab materials such as needles and blood or tissue collection implements must be stored in such a way that the investigator is able to demonstrate the safe, controlled, and sterile condition of materials at all times.
    - If applicable, records of training or license to use lab materials must be maintained by the investigator.

- Non-Controlled Substances:
    - Investigators must develop a protocol for purchasing, constitution, use, and disposal of agents and substances. This protocol should include a plan for documentation of receipt and disposition of all substances.
    - Nutritional supplements and placebo agents must be stored in such a way that the investigator is able to demonstrate the safe, controlled, and sterile condition of substances at all times.
    - Local anesthetics are not listed as a controlled substance in MO, but must be kept in a secure location with access limited to key members of the research team responsible for their use. An open lab or similar high traffic area is not an appropriate area to store such materials.
    - An access log with name, contact information, signature or initial, and dates of access must be kept for each study involving agents or substances.
    - If applicable, records of required training or license to use or dispense an agent or substance must be maintained by the investigator.