LSU Health
NEW ORLEANS
Human Research Protection Program

RESEARCH DATA PROTECTION PLAN

P & P	VERSION DATE	REPLACES P & P	PREVIOUS VERSION DATE
4.06	02.08.2020	5.30	03.25.2019

All human subject's research submitted for consideration by the LSUHSC-NO IRB must include a department approved research data protection plan. In addition, Department Heads and/or Center Directors will be required to provide signature confirmed approvals that the proposed plan is in compliance with federal regulation, institutional information technology guidelines, and LSUHSC-NO IRB policy. The purpose of the plan is ensure research data are appropriately protected from loss or unauthorized disclosure. It should also assure research data can be recovered in the event of a disaster, equipment failure, loss of encryption keys, and theft or loss of research equipment.

The LSUHSC-NO IRB Chair or designee will review and evaluate all research data protection plans. This evaluation will be completed during the initial review consideration of the research and periodically throughout the study approval period. It will also be the LSUHSC-NO Chair's discretion to audit individual approved plan for routine review of for–cause.

The plan proposed by a Principal Investigator to the LSUHSC-NO IRB must address the following components related to the research and working environment of the research team:

1. List and describe all locations where the original and any copies of the data will be kept (and provide building name, street address, and room numbers).
2. Describe the computing environment in which the data will be used, including:
    - Computing platform (e.g., personal computer, workstation, mobile or portable device) and operating systems
    - Number of computers on which data will be stored or analyzed
    - Whether devices used in the research project will be on a network or will be stand-alone.
    - Physical environment in which computer is kept (e.g., in room with public access, in room locked when not in use by research staff)
    - A list and description of all devices on which data will be stored (e.g., network server, One Drive for Business, storage device, PC hard drive, removable storage device such as USB hard drives, USB flash drives, SD cards and other memory cards, CDs, DVDs, etc.)
    - Methods of data storage when data are not being used
    - Methods of sanitation of equipment used in the study when no longer needed
    - Methods of transmitting the data between research team members (if applicable)
    - Methods of storage of computer output both in electronic form and in hard copy (on paper or other media)
    - Recovery plan to be implemented in the event of loss of data due to natural disaster, equipment failure, loss of encryption keys, loss or theft of a device, etc. and
    - Instruction in data protection policies that will be provided to each staff member and student before they receive access to the data as well as recurrent instruction that will be conducted at least annually.

Although LSUHSC-NO Principal Investigators are encouraged to suggest a variety of components for their research data protection plan, all plans approved by the LSUHSC-IRB must include some or all of the following features:

1. Password-protected access to all devices storing the data
2. Automatic activation of password-protection after five minutes of inactivity on the computer
3. Encryption of all files containing Protected data stored on devices other than LSUHSC-NO servers or One Drive for Business (identify encryption software to be used e.g. Bitlocker, PGP, Veracrypt, etc.)
4. No storage of the data on laptop computers, unsecured network servers, etc. without encryption
5. Secure storage of any and all removable devices holding the data (e.g., USB hard drives, USB flash drives, SD cards and other memory cards, CDs, DVDs, etc.), through encryption and storage in a locked compartment or room when not in use
6. Storage of detailed printouts derived from data analysis in a locked compartment or room when not in use
7. Shred all detailed listings and printouts that are no longer needed
8. Prepare and maintain a log of all data files acquired. Record dates that data and paperwork are received and returned or destroyed
9. Protect all files containing Protected and/or Restricted Data in accordance with the Data Protection Plan and destroy or otherwise render the Protected and/or Restricted data unrecoverable once it is no longer needed by the research team
10. Report any and all violations of the Data Protection Plan to the IRB and the Compliance Officer
11. No transmittal of data or detailed tabulations via email or email attachment over the Internet without ensuring that the recipient supports encrypted transmission. Data can also be transmitted by LSU Health Files.
12. Brief all research staff that have access to Protected Data about the Data Protection Plan, appropriate safeguards, and penalties for inappropriate use.