The University of Mississippi

Electronic Human Subjects Data Security

Summary/Purpose: Data Security requirements for human subject data that are both identifiable and sensitive.

The University of Mississippi extends NIH policy (Notice Number: NOT-OD-08-066) regarding data security to all IRB-approved projects and expands coverage to all electronic storage devices, including cloud services. Researchers must protect electronic sensitive, identifiable data (ESID) from disclosure, release, or loss from theft or breaches in data storage or transmission.

Definition of Sensitive Information

Sensitive information is information which, if disclosed, could place research subjects at risk of criminal or civil liability or damage subjects' financial standing, employability, or reputation.

Sensitive information includes but is not limited to:

- mental health survey or interview data
- sexual behaviors
- illegal drug use
- medical diseases
- financial information
- Political or religious beliefs
- Health habits

Potential non-sensitive information data examples include:

- innocuous attitudes
- physical performance

ESID Storage Requirements

ESID must be stored using one or both of these methods:

1. Physically separate data from identifiers
   a) Record data on one storage device
   b) Add a code number to each subject
   c) Copy the code and move the identifying data to a separate device
   d) Keep the two devices physically apart (never carry or store a laptop and thumb drive together)

2. Encrypt the data. See *Data Encryption Guidance & Requirements* below.

Transmitting ESID Electronically (e.g., email)

Transmit ESID electronically only if the ESID is encrypted.

Cloud Storage

ESID stored on cloud services must follow ‘ESID Storage Requirements’ above

Data Encryption Guidance & Requirements

Free, user-friendly encryption software recommended by IT is available at https://itsecurity.olemiss.edu/tools.html

Encryption requires creation of a password and/or certificate to access your encrypted data. Loss of access keys means data can never be recovered. Inaccessible human subjects data alters the cost-benefit ratio IRB evaluates in reviews, because the benefit from new knowledge is lost. Therefore, to reduce this risk, **investigators who encrypt data must also back up their data using method #1 above.**

Related policy (IT): Information Confidentiality/Security
https://secure4.olemiss.edu/umpolicyopen/ShowDetails.jsp?istatPara=1&policyObjidPara=10654991