Adjust your audio settings here.

Type all your questions in the Q&A space (not in the chat window). We will answer all your questions at the end of the webinar.
Best Practices for Managing Human Research Data
Objectives

• Cover the IRB’s scope regarding human research data management
• Present expectations for collecting and sharing data
• Review policy on secure data storage
• Explore “lessons learned” with mismanagement of data
• Provide clarity on the documentation required for sharing
Authority and Scope of the Emory IRB

§46.111 Criteria for IRB approval of research:

- “When appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.”
Collecting or Sharing Human Research Data
Security Review

If using protected health information (PHI), individually identifiable health information (IIHI), or sensitive information (e.g. drug use, alcoholism, sexual preferences) and the data set contains identifiers, security review may be required.

The security review process involves an assessment of potential risks related to the method of sharing the data. This review is conducted by the Office of Information Technology (OIT) and is done in addition to the IRB review.

*For studies taking place and Children’s Healthcare or Grady sites, security review will be completed by their respective privacy offices*
“Vetted” Options for Human Research

Emory OIT approved apps for research:
Find a complete and updated list on the OIT website

Emory Zoom Account Type (PDF):
HIPAA-compliant vs. General (also on the OIT website)
Basic Protections

• If data is coded and stored without identifiers, then basic security protections will apply. The IRB will inform if any changes are needed to the proposed plan.

• As noted previously, there is guidance available on the website for when security review is required.
Sharing Data

Email encryption is required if emailing sensitive information to people outside Emory or consents (even if empty) to study participants.

FAQs around encryption
Emailing Data

**WHAT TO DO**

- **To**: example@university.edu
- **Cc**
- **Subject**: (encrypt) OR (secure) Subject

**WHAT NOT TO DO**

- **To**: example@gmail.com
- **Cc**
- **Subject**: consent and medical info
Securing Data

- Use encrypted devices for storage
- Keep hardcopies of research files in locked cabinets in secured locations
- ONLY share with recipients that are approved to access the data.
  - For example:
    - IRB approved study team members
    - Sponsor representatives
    - Compliance staff
IRB Protocol Requirements:

Include a statement reflecting compliance with Emory’s Data Security Policy. All sensitive data and data that contains HIPAA identifiers, when electronic, must be stored on a hard drive, disk, or thumb drive that is encrypted – not solely password-protected or kept in a locked office.
Protocol Details

Plan to protect the privacy of subjects and confidentiality of data and/or specimens. The plan needs to answer the following questions:

- What identifiers will be kept with the data?
- If codes, where will the key linking the codes to identifiers be kept? Will other parties help create and/or host the database? How will data be securely stored?
- Will other parties help with statistical analysis, and if so, will identifiers be removed first?
- What are plans for protecting the data or disposing of it once the study is completed?
Securing Data

WHAT TO DO

WHAT NOT TO DO
Consent Terms

• Be clear on what will be shared and the purpose of the disclosures

• Include a statement on plans for maintaining confidentiality
Other Devices:

- Make sure to familiarize yourself with any device that is capable of transmitting data, even if that is not your intent.

- For example, video recording devices can be configured out of the box to connect to available networks. Make sure you update the setting to not connect, since it’s not possible to know where data is transmitted once online.
Data Transfer Agreements (DTA)

- Data Transfer Agreements (DTAs) are used to transfer human subject data from one institution to another for research purposes. A DTA is a contract between the providing and recipient institutions that governs the legal obligations and restrictions, as well as compliance with applicable laws and regulations, related to the transfer of such data between the parties.

- The Office of Technology Transfer (OTT) can assist with this process.
The NIH Data Management & Sharing (DMS) Policy, effective January 25, 2023, applies to all research, funded or conducted in whole or in part by NIH, that results in the generation of scientific data.
Elements of NIH Plan

- Data Type
- Related Tools, Software, and/or Code
- Standards
- Data Preservation, Access, and Associated Timelines
- Access, Distribution, and Reuse Considerations
International Data Policies

- **GDPR:** The General Data Protection Regulation (GDPR) standardizes data privacy laws across Europe and puts in place more robust protections for individuals whose personal information is stored and maintained by any organizations.

- **PIPL:** China has a Personal Information Protection Law (PIPL), which applies to the processing of personal information of individuals living in mainland China on or after November 1, 2021.

- Any questions? Reach out to our colleagues in the Office of Compliance at https://compliance.emory.edu/
Lessons Learned

- Don’t blind copy (bcc) when sending emails to participants
- Double check your recipients list! Also, it’s best to cut and paste from a trusted source
- Contemplate strategies for avoiding fraudulent response with online surveys
- Redact information that is uploaded in the eIRB system
Contact Us

Emory IRB

irb@emory.edu

404-712-0720