Data Storage and Security Checklist

- □ What data do we need to store during our active project?
    - Physical, Electronic
    - Sensitive, De-identified
- □ What is the expected size of the data we need to store? How much storage do we need?
    - Electronic
        - How many participants?
        - File size?
    - Paper
        - Number of physical papers/books/etc.?
- □ What are our requirements? How do we stay compliant?
    - IRB requirements
    - Institutional data policies
    - Funder DMP
    - Organizational IT Department policies
    - FERPA, HIPAA
    - Confidentiality
    - What are our data classification levels (DCL)?
- □ What are our secure storage solutions?
    - Electronic (consider hardware and software)
    - Physical
- □ Are there any costs associated with our storage solutions?
- □ How will our storage be structured?
    - Electronic
        - Do we have a file structure laid out in a Style Guide?
        - Do we have file naming conventions laid out in a Style Guide?
    - Physical
        - How will physical data be organized?
    - Who will build these structures?
- □ Who will have access to what? How are permissions set?
- □ How will data be backed up?
    - What tools will be used?
    - How often will backups occur?
    - Who oversees the backups?
- □ How will we document data storage and security rules?
- □ How will staff be trained on data storage and security rules?
    - Who trains staff?
    - What is the frequency of training?
- □ Will there be a data use/access agreement for staff?

  - Who will draft the agreement?
  - How will agreements be collected?
  - What will the oversight of this look like?
- □ Who will monitor data storage and security?
  - Data is being stored securely
  - Update permissions as needed (ex: when staff leave access is removed)
  - Monitor training compliance

Transfer

- □ If we need to transfer data, how can we do so securely?
  - How will paper data in the field be returned to the office in a way that protects confidentiality?
  - How will paper data in the field be protected so that data is not lost?
- □ How are team members allowed to share data?
  - How will electronic data be securely shared with partners at other sites?
    - This could be sharing study data with project partners at other universities or sharing rosters with school sites. How should they plan to share study information securely that doesn't comprise participant confidentiality.

Internal Data Use

- □ How can data be used internally?
  - How can team members access data for analysis?
  - What data are team members allowed to use for analysis?
  - Who oversees this process (of team members using study data)

Retention

- □ How long will we retain our raw data?
  - What is required to be compliant?
- □ How will we dispose of data when we need to?
  - Electronic
  - Physical