Protecting Participant Privacy and Confidentiality in Research

Michael Lawrence, MS

Assistant Teaching Professor

Assistant Program Director

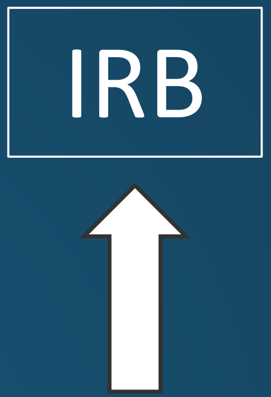
Department of Physical Therapy

OBJECTIVES

- Define common terms
  - Human subject
  - Intervention
  - Data
  - Privacy
  - Confidentiality

- Review standards for maintaining privacy and confidentiality

- Review best practices for data management



IRB

IRB reviewers are likely to focus on these sections

Common Terms

1) Human subject (45 CFR 46.102(e))
    1) Living individual
    2) Researchers use to gain information or biospecimens through interaction/intervention
    3) Researchers obtain, use, study, analyze, or generate identifiable private information/biospecimens

2) Intervention (45 CFR 46.102(e))
    1) Procedures used to gather information
    2) Manipulations of participant or participant's environment

Common Terms

IRB

1) Private Information (45 CFR 46.102(e))
    1) Information provided for specific purpose
    2) Participant can reasonably assume information will not be made public
    3) Any recording/observation/sharing must be included in informed consent documentation

2) Identifiable Private Information (45 CFR 46.102(e))
    1) Participant identity readily ascertained by investigator or associated information

Examples:
Name, address, email, birthdate, video, etc.

Common Terms

IRB

3) Non-identifiable information
    1) Typically information collected for analysis
    2) Not likely to identify participant if a breach were to occur
    3) Depending on population, some of this information may need to be reclassified as identifiable
        1) Small or well known populations
        2) Information that can easily single out an individual

Examples:
Age, height, weight, political affiliation, etc.

Privacy vs. Confidentiality

Privacy

- Right to control access to ourselves
- Applies to the person
- Focus on interactions with participants

Areas to focus

- Description of research environment
- Includes attaining consent
- Methods for allowing participants to limit information shared

Confidentiality

- Agreement of how data will be managed
- Applies to information
- Focus on data management practices

Areas to focus

- Storage of data after collection
- Data transportation/transmission
- Who has access to data
- Destruction of data

Privacy

IRB

- Maintained from recruitment throughout all research activities
- Always consider the environment of the interaction

- Recruitment
  - Do not ask for volunteers to identify themselves in front of a group
  - Provide contact information for participant to reach out to researchers

- Research activities
  - Describe the space and safeguards to protect privacy
    - "Only those on the research team will be allowed in the lab during data collection"
  - If in public space, be sure not to collect private information

Privacy

IRB

- Interviews
  - In person
    - Private room where no one can hear responses
    - If others must be present (focus group) ensure private information is protected
      - Vegas Rule – 'What happens in focus group stays in focus group'
  - Zoom
    - Allow participants to disable their camera/change screen name
    - Use a private link that is not accessible to others
    - Use the passcode feature

Data Confidentiality

IRB

- Storage & Security
  - Describe the format of the data (e.g. paper or electronic)
  - Describe the location data will be stored (file cabinet, laptop, cloud, specific software, etc.)
- Accessibility
  - Who needs access to data
  - Who needs to access consent forms?
- Sharing
  - Method and security?
- Destruction
  - When will each type of data be destroyed?
  - Consent forms must be kept for at least 3 years after completion of study
  - Private identifying information – destroy as soon as reasonably possible

Best Practices - Data storage

IRB

- Electronic folders and files should be password protected
    - Sensitive information (e.g. Identifiable information) should be encrypted
- Hard copy files should be in locked drawers/cabinets
- Store identifying information (e.g. Master list or key) separate from study data
    - Identifying documents are best stored in a hard copy
- Avoid storing any information on portable devices
    - If necessary, encrypt the disc/device

Best Practices - Data Accessibility

- Restrict access to only those who require it for their role in the study

- Typically only the PI has access to signed informed consent documents

Best Practices - Data Sharing

IRB

- Data should only be shared by entity that originally collected it

- If transmitting identifying information
  - Data itself should be encrypted
  - Use encrypted communications medium

- Any sharing of data should be mentioned in the informed consent documentation
  - Sharing with other institutions
  - Posted to data repository (NIH funded studies)

Best Practices - Data Sharing

IRB

- Unacceptable software options
- Google accounts (Gmail, google docs, etc.)
- Survey monkey
- Personal email accounts/drives

- Some acceptable software options at UNE
  - REDCap
  - Qualtrics
  - BOX
  - UNE network drives
  - UNE Onedrive/Sharepoint

Best Practices - Data destruction

- Consent forms must be retained for at least 3 years after study completion
- Should destroy identifying information as soon as possible
- It is acceptable to retain de-identified information indefinitely
- All of this information must be in the informed consent documentation

Best Practices for Data Management

1. Collect only data needed for the study

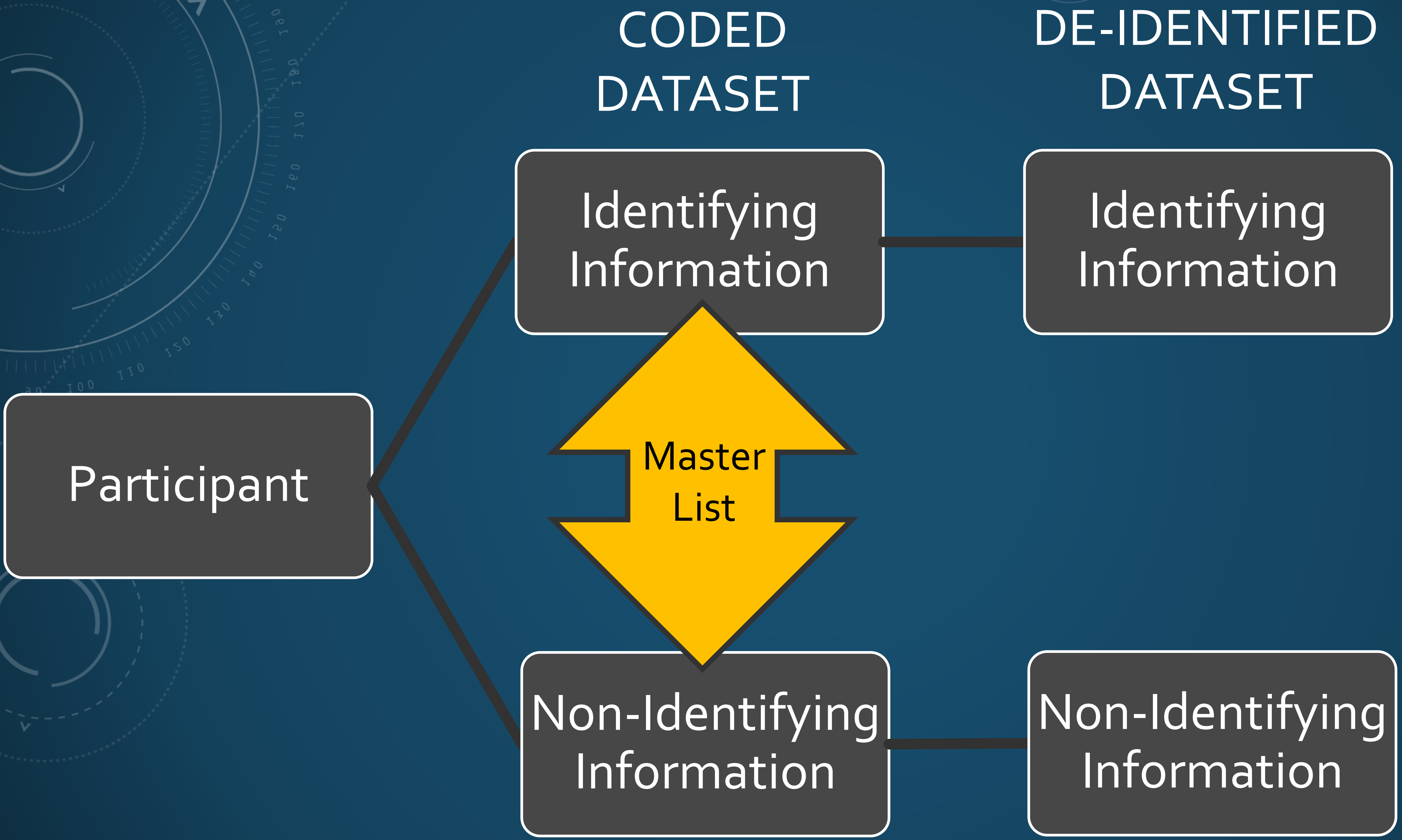
2. If possible de-link data from participant identity

Collect only Data you Need

- Should be able to link each data to research or logistical need
- What's needed for the purpose of the study?
    - Example: Birthdate or age?
- Logistical Need
    - Participant contact information for scheduling

De-linking data

- De-identified
  - Not able to readily re-identify participants
- Coded
  - A unique participant code used to link participant identify and data
  - Can create a de-identified data set by destroying the link between the code and identity
- Anonymous
  - No way to ever link participant identity to data
  - Researchers are never aware of the identity of their participants



CODED DATASET

DE-IDENTIFIED DATASET

Participant

Identifying Information

Master List

Non-Identifying Information

Identifying Information

Non-Identifying Information

Master List

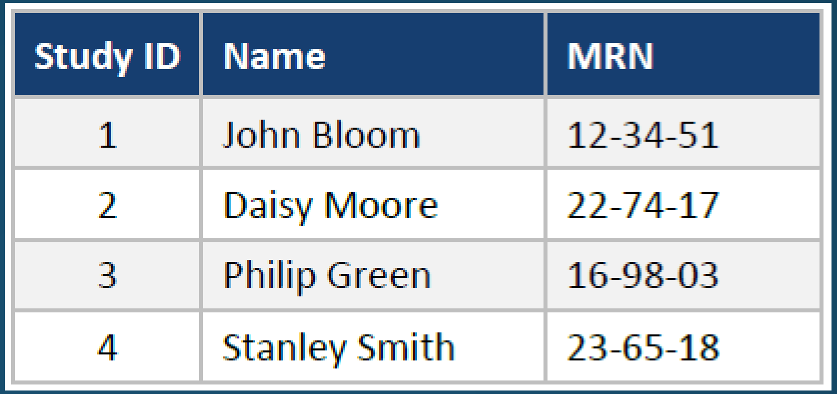
IRB

- Links participants to their unique code
- May contain contact information
- Must be stored in a secure location different than where study data is stored

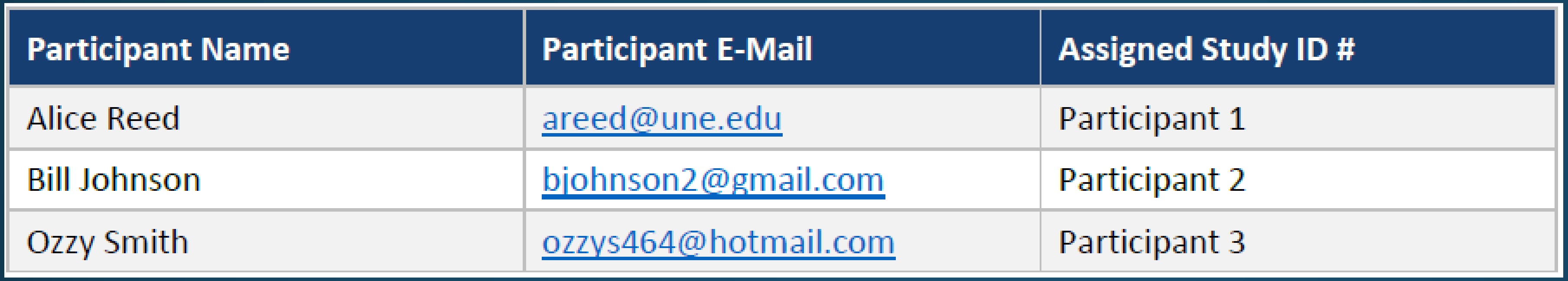
Guidance for Master List: https://www.une.edu/research/integrity/irb

- Best Practices
  - Store as a hard copy in a locked file cabinet
  - Do not store on mobile devices unless absolutely necessary
  - Destroyed at earliest opportunity
  - Restrict access to only those who require it

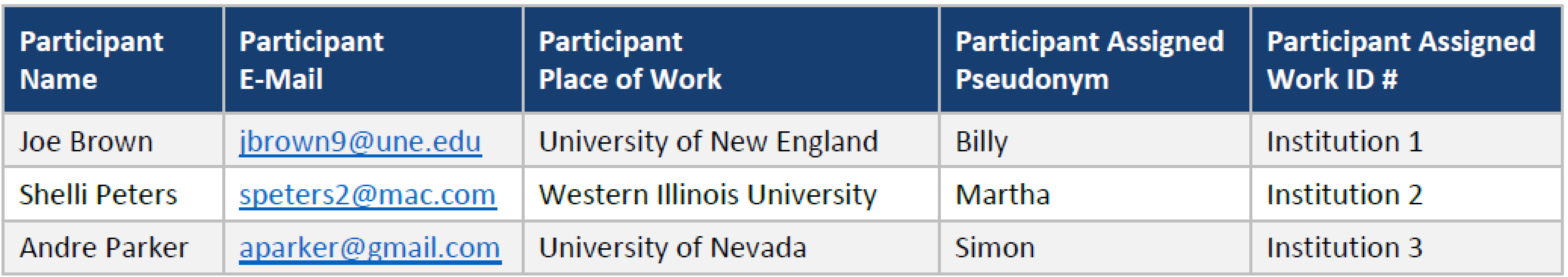
Master List Examples



Study ID	Name	MRN
1	John Bloom	12-34-51
2	Daisy Moore	22-74-17
3	Philip Green	16-98-03
4	Stanley Smith	23-65-18



Participant Name	Participant E-Mail	Assigned Study ID #
Alice Reed	areed@une.edu	Participant 1
Bill Johnson	bjohnson2@gmail.com	Participant 2
Ozzy Smith	ozzys464@hotmail.com	Participant 3



Participant Name	Participant E-Mail	Participant Place of Work	Participant Assigned Pseudonym	Participant Assigned Work ID #
Joe Brown	jbrown9@une.edu	University of New England	Billy	Institution 1
Shelli Peters	speters2@mac.com	Western Illinois University	Martha	Institution 2
Andre Parker	aparker@gmail.com	University of Nevada	Simon	Institution 3

Additional Resources

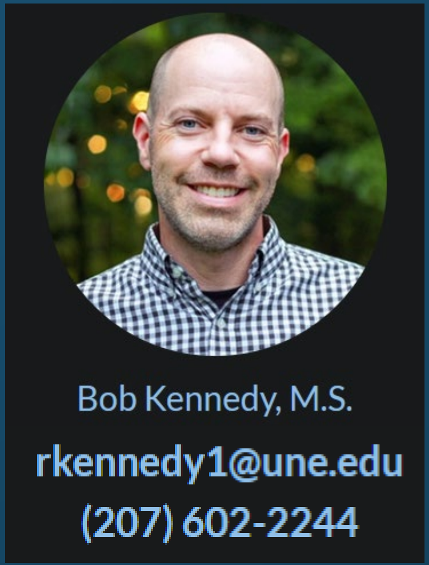
Federal Guidelines (Common Rule)

https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/index.html

Boehnen, C., Bolme, D., & Flynn, P. (2015). Biometrics IRB best practices and data protection. Paper presented at the *Biometric and Surveillance Technology for Human and Activity Identification XII, 9457* 94570F-7. https://10.1117/12.2181981 http://www.dx.doi.org/10.1117/12.2181981

UNE IRB website

https://www.une.edu/research/integrity/irb



Bob Kennedy, M.S.

rkennedy1@une.edu

(207) 602-2244