Ensuring Protection of Study Participant Personally Identifiable Information (PII)
Katie B. Speanburg, EdM; Sean Owen
Abt Associates

Submission Type: Programmatic
Topic Area: Education and Training
Poster Number: 19

Background: Our institution conducts social-behavioral research and evaluation with several hundred Federal government grantees and sub-contractors at any one time. While many aspects of the partnerships are successful, our partners struggle to consistently follow the security procedures required to protect participant data. For example, PII that our organization is authorized to receive has been emailed to us un-encrypted, paper with PII is misplaced for several months, and non-participant data has not been excluded from our cohorts’ datasets!

Methods: Our IRB has partnered with our Information Security and Contracts Departments to create strategies to reduce these risks that include 1) explicit security requirements in contracts and data agreements; 2) training of partners on data security procedures and responding to incidents; and 3) procedures to protect research participant data while stored and in transmission. Our program targets three key areas of security in program implementation, starting with the contract and data agreements. We have required language built into our sub-contracts that describes the required data security procedures such as transferring data via secure web portal and encrypting data. The subcontract also defines the expectations we have if participant data is lost. We then conduct in-depth in person training for all partners who handle research participants’ PII. The training reviews the project specific procedures to be followed as well as the background, history, and purpose of data security using real examples of data breaches and the consequences. At the end of training, staff sign Individual Investigator Agreements to pledge their commitment to the procedures they have learned. For longitudinal studies, we conduct low-cost refresher training to reinforce the importance of data security via webinars, bulletins, tailored posters, and focused 1:1 re-training as needed.

Evaluation: To make the secure transfer of PII easy, we have set-up a user-friendly portal and provide clear guidance on using the portal. Internally, we systematically track all PII carefully using data security plans, several methods of checks and balances, and quick incident response if it appears PII has been disclosed or misplaced. Evaluation measures include number of partners trained, reduction in security incidents, and reduction in disclosure of PII. Grantees and sub-contractors can implement the data security practices in their own organizations to strengthen the protection of their own program clients’ PII. Our organization and others like ours can implement these strategies company-wide and build strong data security cultures.