Creating Data Security Guidance and Policy at the University of California, Berkeley
Colleen Kohashi, MA, CIP; Adrienne Tanner, CIP; Tani Prestage, MPA, MA, CIP; Dragana Nikolajevic, MPA, MSc
University of California, Berkeley

Submission Type: Programmatic
Topic Area: Regulations and Guidance
Poster Number: 95

Program Statement: In 2012, our IRB was faced with the task of revamping its antiquated data security policy dating back to 2005. With the advent of new technologies, the way that researchers conduct their research and store their data (particularly online) has drastically changed in recent years. Given the importance of data security in research, it was clear that our IRB needed to have up-to-date data security policies with which to guide our research community. Generally, our IRB bases its policies on the Office for Human Research Protections’ requirements. However, because there are no national-level data security specifications for IRBs, we instead took advantage of other resources. We turned to our IRB Committee members with data security expertise and the campus IT security department, as well as publicly available policies from other R1 institutions. This poster will shed light on our experience with creating an institutional data security policy, along with its challenges and successes.

Description of the Program: The main goal of the revised policy was to put forth information on protecting subjects’ identifiable data that was accurate and up-to-date as well as accessible. In March 2013, after many different iterations and modifications, we launched a new data security policy, as well as a data security guidelines matrix. The matrix is organized by data sensitivity level and displays corresponding data security protections. The goal of the matrix is to supplement the policy by providing pertinent data security information in a visual fashion in order to assist with comprehension. Our IRB staff uses these documents to educate our campus’ research community and as a basis for the data security requirements in our IRB applications. Moreover, in order to better reflect our new policy, our IRB is almost finished overhauling the confidentiality questions within our IRB applications as well.

Suggestions for Implementation: When updating our data security policy and creating guidance, it would have been helpful to consult with other institutions regarding their experiences with such processes. As it was, we were very lucky to be associated with a large institution where there were many resources and experts with whom we could consult. We recognize that many smaller institutions don’t have the same ability/resources. We propose to document the process of creating a data security policy and matrix at our institution in the hopes that it will aid other IRBs as they attempt to meet the needs of their own research communities.