Guidance on Protecting Research Data

Chaminade University IRB
September, 2015.

Protecting Research Data
In social and behavioral research, breach of confidentiality is a serious risk posed to research subjects. Rigorous data security is a key element of protecting subject data from an accidental or malicious breach. Data security includes a plan to manage the physical documentation associated with the project, such as paper surveys, signed consent forms or documents that contain contact information for subjects, to insure that those materials are not lost or accessed inadvertently by an unauthorized person. Increasingly important is the management of electronic data on desktops or servers as well as on mobile devices such as laptops and flash-drives.

Protecting this important data requires a commonsense approach to managing your computer systems. All university researchers need to be aware of common vulnerabilities and then take necessary steps to shield those vulnerable areas.

An important component in the IRB approval process is whether adequate provisions exist for the security of research data. When conducting research, investigators are entrusted with confidential and privileged human subject information, whether in paper or electronic form and must take measures to protect the security of this information. For IRB approval, PIs are required to:

1. Describe procedures (including safeguards for collecting, storing, processing subject data and data destruction) for minimizing potential risks to subject's confidentiality.
2. Specify where and under what conditions individuals will have access to the data, what will be available and to whom.

Please consider the following when preparing your IRB application:

1. The IRB expects researchers to access only data that are necessary to conduct the study. Collect only minimum necessary information. Social security numbers and full birth date (mo/day/year) are protected information that generally should not be collected.
2. In the informed consent document, PIs must describe protection and confidentiality of records.
3. Keep data at a secure location. A secure location is a place to which only the PI and authorized research staff have access.
4. Limit electronic access to any computer that contains subject identifiers by password protection. Avoid storing data on portable devices, as these

devices are susceptible to loss of theft. If the PI needs to use these devices, remove identifiers from data files and associate them with codes kept in a separate location. The data should be encrypted.

5. Avoid storing subject identifiable data on portable devices (such as laptop computers, cell phones, digital cameras, portable hard drives including flash drives, USB memory sticks, iPods or similar storage devices), as these devices are particularly susceptible to loss or theft. If there is a necessity to use portable devices for initial collection of subject identifiers, the data files must be encrypted, and subject identifiers transferred to a secure system as soon as possible.
6. If subject identifiers will be retained in the data files because of the specific needs of the research study, additional justification must be provided by the Investigator to justify retention. Again, if the data are stored electronically the files must be encrypted.
7. Use only secure modes of transmission of data; data submitted over a public network should be encrypted.
8. If there is an unanticipated breach of confidentiality of the research data, the PI must report this to the IRB within 5 business days of becoming aware of the event.

Adapted from University of Notre Dame IRB Guidelines, 2015