Guidance for the Safe Storage and Management of Research Data

February 1, 2016

The IRB recognizes that research involving human subjects conducted by investigators at William Paterson University can occur in many different ways and locations. It can be conducted by students, faculty and staff as well as by outside investigators. Students, in particular, may be working with a significant level of independence or may be closely supervised in a lab or clinical setting. Because of this great variety, the IRB has established the following **recommendations** regarding the safe storage of data that conveys its core concerns about protecting access and subject anonymity as well as the flexible implementation related to the particular situation of the research.

A detailed data protection and storage plan must be included in every protocol submitted to the IRB. Investigators may offer alternative plans to what is recommended in this guidance but must include a justification for the alternative.

A. Basic Considerations for All WP Investigators

- Data must be stored in a secure location with limited or controlled access by anyone other than the investigator.
- Signed consent forms to be kept separately from the original data and any forms of the data that are not anonymized.
- Data stored electronically must be on a password protected *desktop or network* computer or a password protected external hard drive. This applies to data that DOES or DOES NOT include identifiable personal information. Campus computers and network storage drives are password protected and safe for data storage.
- The use of "cloud drives" is discouraged for long-term storage of data but could be allowable if (a) the data is a de-identified copy of the original data that is stored on a secure computer, (b) the level of password protection is considered highly secure (a 13+ character password using upper and lower case letters, numbers and symbols), and (c) there are a small number of individuals with access to the data.
- Laptop and tablet computers, flash drives (aka: thumb, memory card, memory stick), cloud drives and other portable memory devices should only be used for the temporary storage of data. The device or the files should be password protected. This data should be transferred to a password protected computer or hard drive at the investigator's earliest opportunity.

B. Additional considerations for WP Faculty, Staff and Doctoral Students

- All Basic Considerations apply.
- For doctoral students, original data and consent statements may be stored at home in a manner that meets the Basic Considerations.
- For faculty and staff, original data and consent statements should be stored on campus.
- Copies of data can be stored at home or in other locations in a manner that meets the Basic Considerations.
- When data sharing is required by a sponsor of the research, or if data is voluntarily shared with other investigators, the data provided must be anonymized.
- For published data: data should be stored for a period of not more than 3 years following the publication of the last article.
- For unpublished data: the data should be stored for a period of not more than 3 years after when the investigator considers the research to have been completed or terminated.
- *Original data with identifiable personal information should be destroyed when it no longer has to be retained. Paper records should be shredded; WP's Storeroom provides shredding services, call them for details. Electronic records should be deleted from all computers and storage devices; this should also include backup files as practical.*
- The data storage requirements of (a) sponsors who are supporting the collection and sharing of data, (b) publishers, or (c) organizations that provide access to data or datasets (paid or free) must be respected and followed even if they contradict these guidelines. *If this is known when the protocol is submitted, this should be included in the protocol. If this is learned after the protocol has been approved, this should be communicated to the IRB as a change using the Continuing Review process.*
- *When the research is part of a multi-site project, the protocol should be clear in indicating which institution will be responsible for storing data and, if it is not WP, to provide a summary of the data storage plan.*

C. Additional considerations for WP Undergraduate and Master's degree students

- All Basic Considerations apply.
- For undergraduate or master's degree student research that IS NOT REVIEWED by the IRB, the professor will be responsible for approving and monitoring data use as well as the destruction of original data at the end of the semester course.
- For undergraduate or master's degree student research that IS REVIEWED by the IRB, the professor will be responsible for insuring that the plan for destroying data included in their student's protocol has been completed.
- Students may keep a copy of the aggregated, de-identified, anonymized data after the course.

D. Outside Investigators

A data storage and protection plan must be included in the protocol approved by the investigator's host institution or a plan must be provided in the submission to the WPU IRB. The WPU IRB expects that other intuitions will have different rules or requirements concerning the safe storage and management of data. An outside investigator's host institution's rules and requirements will be the standard for that investigator's protocol.