Data Storage

Privacy and confidentiality of information is important to minimize the risk to subjects involved. Whether information is kept in electronic, digital, or paper format, it must be secured through administrative, physical and technical protections and accessible only to appropriate persons. Assessment of the adequacy of the administrative, physical and technical protections should include consideration of the sensitivity of the data.

Research records are identified in the University of Arizona Common Records Retention and Disposition Schedule. A record generally is defined as information in any format associated with a research project.

Records to be maintained include: copies of all research proposals reviewed, scientific evaluations (if any), consent documents, progress reports, reports of injuries to subjects and other unanticipated problems, and copies of all correspondences between the IRB and the investigator(s). Records may be preserved in hard-copy, electronic or other media form, and must be accessible for audit purposes. Records for completed projects should be stored in secure locations on campus with the same care used when the project was active.

Paper Records (e.g., consent forms, data files, medical records, etc.): Paper files related to human subjects participation in research must be securely stored on campus. Access to files should be restricted to key personnel and supervised by the principal investigator(s) of the study. Locked file cabinets ought to be used and preferably located in secured locations (i.e., locked office or laboratory). In the event that research activities are not carried on campus AND it is necessary to maintain the consent forms at the research site, copies of the signed consent forms should also be stored on a secure University location (either as a paper copy or in digital form).

Signed informed consents must not be used as the identifying link to the research data and must NOT contain participant ID numbers, nor be filed with other research data files. Consents should be kept in a separate location than the study data itself.

Digital Records (e.g., electronic files, digital recordings, etc.): Digital files containing human subjects research data must be stored in password protected files, preferably on University maintained servers with regular and secured back-up. Sensitive data should also be encrypted.

Tapes and other media-supporting devices used for audio and/or video recordings should be stored in the same secure manner as paper records and erased as soon as information has been transcribed or coded and is no longer needed for research.
Security Provisions

Human Research records varying levels of security depending on the level of risk, type of information collected, and the level of consent obtained from subjects. The University of Arizona maintains security guidelines that investigators should use when storing research data: security.arizona.edu.

HSPP recommends implementing the following practices:

- Backing up all data and storing backups in a location separate from the original.
- Securing all computers (workstations and servers) and storage devices with locks.
- Protecting all computers and electronic media with "sign-on" passwords.
- Using encryption software to encode patient data.
- For Microsoft Windows users, install the latest updates at www.windowsupdate.com.

Encryption

Data encryption transforms plain text files into a format that prevents unauthorized users from opening the files and reading the contents. There are two types of encryption that should be considered: data at rest, and data in transit. The former protects stored data while the latter protects data as they are being transmitted between parties over a public network. Unless otherwise specified by the IRB, it is recommended that the highest level of data encryption be used, within the limits of availability and feasibility.

Project Closure and Record Retention

Approved human subject research projects should be closed at the time all data have been collected and identifying information is no longer needed. De-identified data for which no identifying key exists can be kept for further analysis and do not require continuing review and approval by an IRB.

If a researcher (faculty, staff or student) leaves the institution, a copy of the research records must remain on campus. Students should coordinate storage of research records with their faculty advisor(s) and/or departments. Arrangements can be made to ship records off to the records archive for long-term storage.

Research records should be maintained for whichever of the following time periods is the longest:
Data Storage and Retention

a) The length of time required by law; or
b) As long as the sponsor requires (for sponsored research); or
c) 6 years after the completion of the research; or
d) 6 years after the age of majority, if the research involves children

For accessibility purposes (such as audit), original, signed consent forms must be kept in a secure location on University of Arizona property. Store research records as described in the IRB approved project. If desired, the investigator may archive these records with UA Records Management.

FDA regulated research

In accordance with FDA requirements, an investigator shall retain records required to be maintained under FDA for a period of two (2) years following the date a marketing application is approved for the drug or device for the indication for which it is being investigated; or, if no application is to be filed or if the application is not approved for such indication, until two (2) years after the investigation is discontinued and FDA is notified.

Destruction of Records

Destruction of human subjects research records should be performed in a fashion that protects the confidentiality of the research subjects. It is recommended that paper records be shredded, that physical tapes (audio and video) be erased and physically destroyed, and that electronic media used to store data be scrubbed after the files are deleted.

Researchers may retain de-identified data for future analysis in the context of the project the data were collected for. Data are considered to be completely de-identified when ALL links between individual identity and the data are destroyed. Research data are not considered de-identified simply because names have been removed if they still contain information that might identify the participants such as date of birth, address, etc.

Any requirements of study sponsors shall not be construed to require less security than indicated in this or any other University data management policy.

The physical storage location(s) should be reasonably secure against theft and loss due to fire, flood, electrical surges, and other forms of physical damage.

Personally identifiable information (e.g., IP addresses, PHI) must be kept separate from the data.

Use of external vendors for data storage and transfer (i.e., cloud storage) is permitted subject to final IRB approval. For data related to studies determined to be more than minimal risk to
participants, the data must be stored encrypted on secure servers, using the SSL/TLS protocol while in transit, and in a secure location in a manner that assures only authorized access to the data, and that no unauthorized changes can be made to the data.