THE UNIVERSITY OF ARIZONA Research, Discovery & Innovation

Data Security and Records Retention

Overview
The University of Arizona takes seriously its commitment to respect and protect the privacy of individuals that participate in research, as well as, to protect the confidentiality of information. The IRB is tasked with ensuring the protection of data and information related to human research protocols.

Data security review
Part of the IRB review and approval is to ensure that identifiable private information or identifiable biospecimens have the appropriate data security standards. The IRB is required to ensure the following:

- The extent to which identifiable private information is or has been de-identified and the risk that such de-identified information can be re-identified;
- The use of the information;
- The extent to which the information will be shared or transferred to a third party or otherwise disclosed or released;
- The likely retention period or life of the information;
- The security controls that are in place to protect the confidentiality and integrity of the information; and
- The potential risk of harm to individuals should the information be lost, stolen, compromised, or otherwise used in a way contrary to the contours of the research under the exemption.

Therefore, as part of IRB review, researchers are required to address these points in the IRB application.

Data classification standards
The University of Arizona Information Security Office has created guidance for researchers to classify data at the university and the storage allowed for such data (http://security.arizona.edu/data-classification-and-handling-standard#classifications).

The categories of data are Regulated, Confidential, Public, and Internal for the purpose of determining who is allowed to access the information and what security precautions must be taken to protect against unauthorized access.

Human Subjects data is considered confidential and HIPAA data is Regulated. Below is a description of the requirements to protect data in these categories:

	Confidential	Regulated
Description	Data protected as Confidential by law, contracts, or third-party agreement, and by the University for confidential treatment. Unauthorized disclosure,	Data controlled by federal, state, local, and/or industry regulations. These data are affected by data breach notification laws and contractual provisions in government research grants, which impose legal and technical restrictions on the

	alteration, or destruction of this data type could cause a significant level of risk to the University or its affiliates.	appropriate use of institutional information.
Examples	- Applicant, alumni, donor, potential donor and parent data - FERPA and GLBA data - Human Subject Research data - Restricted or unpublished research data - Data protected by confidentiality agreements - Law enforcement or court records and confidential investigation records - Citizen or immigrations status - Detailed information about certain University buildings, activities or events, including facility security system details	- Social Security Numbers - Credit Card Numbers - Financial/ Banking Account Numbers - Driver's License Numbers - Health Insurance Policy ID Numbers - Data as defined under FISMA, ITAR/EAR, HIPAA
Access	Access limited to those with a need to know, at the discretion of the data owner or custodian.	Access limited to those permitted under law, regulation and UA policies, and with a need to know.
Transmission-Encryption	Encryption is strongly recommended when transmitting information through a network. Third-party email services are discouraged for transmitting Confidential Data.	NIST-approved encryption is required when transmitting information through a network. Regulated numbers may be redacted instead of encrypted.
Transmission-Wireless Network	Encryption is strongly recommended when transmitting information through a wireless network. Third-party email services are discouraged for transmitting Confidential Data.	Wireless transmission of data must be approved by appropriate compliance officers/and or Information Security Officer. If approved, NIST-approved encryption is required. Regulated numbers may be redacted instead of encrypted.
Transmission-Email	Encryption is strongly recommended when emailing Confidential Data. Third-party email services are discouraged for	NIST-approved encryption is required for all Regulated Data. Third-party email services are not appropriate for transmitting Regulated Data. Regulated numbers may be redacted instead of

	transmitting Confidential Data.	encrypted.
Storage	Encryption is strongly recommended. If appropriate level of protection is not known, check with the data steward and/or UA Information Security before storing Confidential Data unencrypted. Third-party processing or storage services may receive or store Confidential data if UA has a valid contract with the vendor that specifies appropriate storage or Confidential Data.	Encryption is required for storage of Regulated Data. Regulated numbers may be redacted instead of encrypted.

Only certain types of storage mechanisms are allowed for confidential or regulated data as identified below:

Confidential Data

- **Box @ UA** is an online cloud storage and collaboration tool that enables campus users to easily store, access and share files anytime, anywhere, from any device. It is available to faculty and staff for storing or sharing Confidential, Public or Internal data. For more information, go to Box@UA.
- **G Suite for Education** is available for sharing teaching and learning files among faculty and students. For more information, go to the Catmail page.
- **UITS file servers:** Units may contract with UITS to store Confidential, Public, and Internal data on-campus file servers. Colleges, schools and departments may use file servers to manage staff and/or faculty content using mapped network drives, and can designate access on an individual, group, or departmental basis.

Regulated Data

- **REDCap** is a secure web application for building and managing online surveys and forms (or a mixture of the two). Using REDCap's stream-lined process for rapidly developing projects, you may create and design projects using: an online method from your web browser using the Online Designer; and/or an offline method by constructing a 'data dictionary' template file in Microsoft Excel, which can be later uploaded into REDCap.
- **BoxHealth** is a subset of the Box environment that can store HIPAA protected information.

For information or guidance on data classification and handling, please contact UA Information Security at (520) 621-8476 or infosec@email.arizona.edu.

Investigator records

The Investigator is responsible for the maintenance of records related to research projects. Investigator records are intended to be the primary source document and be available for auditing and inspection upon request. For accessibility purposes (such as audit), original signed consent forms should be kept

in a secure location on University of Arizona property. Research records must be stored as described in the IRB approved project.

Record Retention

Research records should be maintained for whichever of the following time periods is the longest:

a) Six (6) years after the completion of the research; or
b) If the research involves children, 6 years after the youngest child in the research reaches the ages of majority (In Arizona the age of majority is 18 years old);
c) The length of time required by law (see below for FDA regulated research); or
d) As long as the sponsor requires (for sponsored research).

If desired, the investigator may archive these records with UA Records Management and Archives (RMA).

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. The sponsor is responsible for notifying the investigator in advance if a marketing application is planned. If no application is to be filed or if the application is not approved for such indication, records must be retained until two (2) years after the investigation is discontinued and the FDA is notified.

Imaging of records

The question most often asked is "Can I scan the signed consents and then destroy the originals?" The answer is yes, but you must meet state standards for imaging. State statute requires that any unit of a State Agency must seek State approval for the imaging program PRIOR to purchasing any hardware or software for the project. If no software will be purchased, the request to scan and store records still must be made.

The request for imaging form can be found on the website for the State of Arizona - Records Management. The request must be submitted through RMA at the University of Arizona. In addition, records retention requirement may exist if the sponsor requires a one year (or other) hold on the hard-copy for audit purposes. RMA can guide the unit through the process.

IRB records

IRB records are retained for six (6) years following completion of the research, which is longer than required by the human subject rules but is consistent with requirements for HIPAA retention.

This applies to all research studies, whether or not participants were enrolled. Sponsored grants and contracts may require additional periods for record retention.