THE UNIVERSITY OF ARIZONA
Research, Innovation & Impact

Data Security and Records Retention

Overview

The University of Arizona takes seriously its commitment to protect the privacy of individuals that participate in research and 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 process is to ensure that identifiable private information or identifiable biospecimens have the appropriate data security standards. The IRB is required to assess 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 documented policies, standards, and guidelines for the classification and handling of information available on their ISO Communications SharePoint site.

University Information has three levels of Sensitivity: Public, Internal, or Restricted.

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

Description

Information has a Sensitivity of Restricted, for any non-Public information for which the corresponding Information Resource Owner has determined any public disclosure poses greater than little risk to the University or University-Related Persons and those that are encumbered by regulatory, statutory, or contractual obligations for confidentiality. It should also be used to designate Information Systems designed to store, process, or transmit information designated as Restricted.

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- Restricted or unpublished research data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

It is important to understand which Compliance Office(s) have oversight and the situations under which notification is needed. Please see Table 1 and Table 2 of the ISO-400-G2 Information Handling Guideline.

Access

“Each individual or role is granted access to the minimum amount of information and system resources needed to perform their job function." ISO-300(B)(1)(b).

Transmission-Encryption

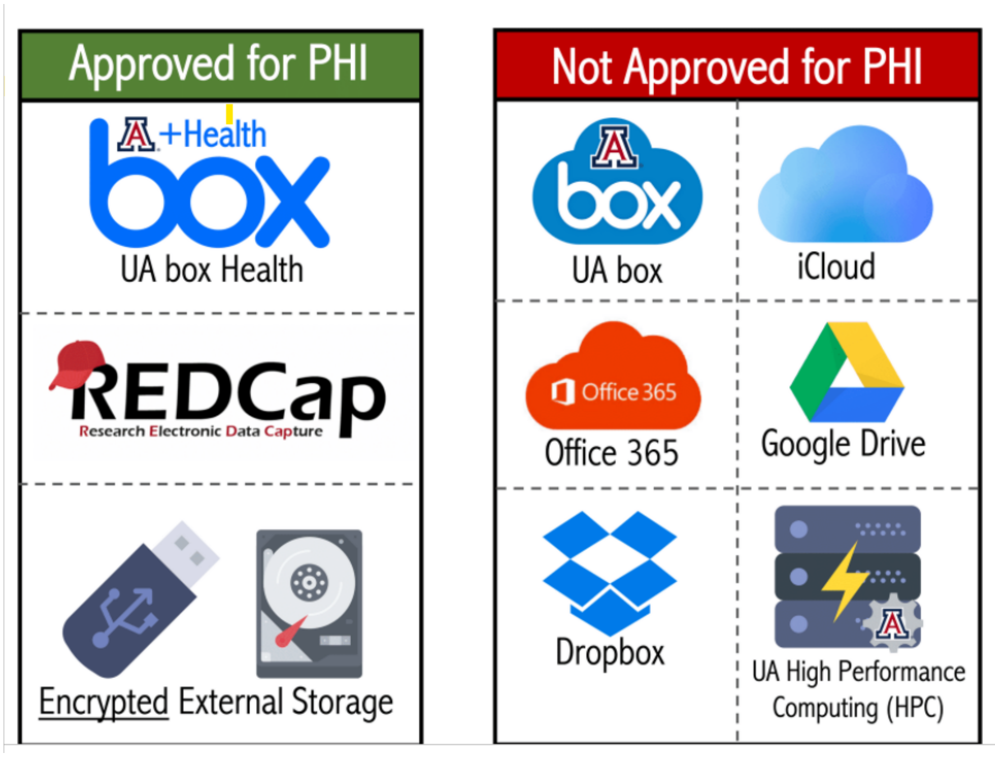
Restricted Information must be: "Encrypted in transit using Transport Layer Security (TLS) version 1.2 or later." ISO-1000-S1(B)(2).

	Examples of encryption in transit include: a) **Email** -- Unencrypted email can be vulnerable to unauthorized or malicious disclosure at a number of points, including on the sender’s device, at sender’s the mail service provider, at the recipient’s mail service provider, or on the recipient’s device. b) **Wireless Access** -- The proliferation of wireless access technology, combined with user carelessness and ignorance, as well as easy, accessible, and sophisticated wireless hacking tools has made wireless communication an attractive target to attackers. It is therefore critical that wireless communications be protected by robust encryption. c) **Remote Access** -- Allows the extension of private networks across a public network, enabling users to send and receive data as if they were directly connected to a private network. In order to ensure security, private network data should only be sent across a public network through a Virtual Private Network (VPN), which uses an encrypted layered tunneling protocol to protect the data. d) **HTTP** -- Hypertext Transfer Protocol (HTTP) is the foundation of data communication for the World Wide Web and is commonly accessed on user devices through web browsers. Hypertext Transfer Protocol Secure (HTTPS) extends HTTP and encrypts the communication using TLS certificates.
Storage	Restricted Information must be: "Encrypted at rest with a cryptographic module that meets the National Institute of Standards and Technology’s (NIST) Advanced Encryption Standard (AES) with a block size of 256 bits and key escrow adequate to provide for third-party data recovery in the event of legal requirements or business need." ISO-1000-S1(B)(1).

Federal regulations and University policy require restricted data (e.g., HIPAA, Export Control, etc.) to be encrypted at certain levels depending on the type of data. The ISO has made their Encryption Guideline available. Please review the Guideline to ensure the proper precautions are taken when working with Restricted data.

Data Storage Platforms

Information Resource Owners are welcome to store Restricted Information anywhere which meets the requirements for Restricted Information. Importantly, when stored or transmitted, Restricted Information must be encrypted, and access must be restricted to only those who "need to know" based on job responsibilities. Recommend storage platforms are identified below:



Additionally, both **OnCore** and **eRegulatory** are approved platforms for PHI storage, and Banner Health has approved **Banner Teams** for instant messaging involving Banner-specific PHI. Note that Banner OneDrive is not an approved platform for storing PHI.

For information or guidance on data classification and handling, please contact UA Information Security.

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. An alternative to storing original signed consent forms may be approved by the IRB. Research records must be stored as described in the IRB approved protocol.

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 agesof 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 & Archives.

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 application for converting paper records to digital scanned records can be found on the UA Records & Archives website. The request must be sent to UA Records & Archives for review and University approval. In addition, a records retention requirement may exist if the sponsor or regulator requires a one year (or other) hold on the hard-copy for audit purposes or other rules surrounding imaging requirements. Records & Archives 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.