IRB Data Security Guidance

Overview

Northern Arizona University 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 and handling standards

Northern Arizona University Information Technology Services (NAU ITS) has created guidance for researchers to classify data at the university and the storage allowed for such data (https://nau.edu/university-policy-library/data-classification-and-handling/). Projects requiring IRB review will be reviewed and assessed against this data security policy.

The four levels of data are 1) Public Data, 2) Internal Data, 3) Sensitive Data, and 4) Highly Sensitive Data for the purpose of determining who is allowed to access the information and what security precautions must be taken to protect against unauthorized access.

IRB Data Security Guidance

Human subjects research data is typically considered confidential and sensitive data. Associated risk depends on the method of data collection(s), the type of participant information and how it is stored.

For information or guidance on data classification and handling for your research, please contact NAU ITS at Ask-STC@nau.edu for students or Ask-ITS@nau.edu for faculty and staff.

Example	Data Class (1-4)	Approved Practices	Prohibited Practices	Comments
US Census public data	1	All.	None (some datasets may require acknowledgement).	Public data can be shared, published, or used without restriction. Data does not fall under IRB oversight.
De-identified human subjects data	1	All except those that could make identification of the data likely	Combining with other data sets that may allow identification.	De-identified or anonymized data is personal information from a medical record that has been stripped of all identifiers—that is, all information that can be used to identify the patient from whose medical record where the health information was derived. Data does not fall under IRB oversight.
Restricted Data Set / Data with indirect identifiers obtained through an external data owner with an	3	Storage on an ITS secured server. Storage on workstation or mobile with full-disk	Storage on USB drive or cd unless encrypted. E-mail of data files.	Many "public data" sets are purchased or provided with restrictions. The data owner requires IRB review and the agreement

IRB Data Security Guidance

Example	Data Class (1-4)	Approved Practices	Prohibited Practices	Comments
agreement that has restrictions		Encryption. Transmission: Encryption required (e.g., TLS or HTTPS or secure file transfer protocols, SFTP, SSH, SMB 3). Cannot transmit via email unless encrypted and secured with a digital signature. All except as prohibited in the agreement.	Use by a person not authorized to use the data Use of the data for a purpose not authorized in the DUA. Per agreement.	restricts access and use.
Limited Data Set (LDS) Obtained from a covered healthcare entity through a data use agreement (DUA)	3	Storage on an ITS secured server. Storage on workstation or mobile with full-disk Encryption. Transmission: Encryption required (e.g., TLS or HTTPS or secure file transfer protocols,	Storage on USB drive or cd unless encrypted. E-mail of data files. Use by a person or for a purpose not authorized in the DUA. Use by a person not authorized to use the data Use of the data for a purpose	LDS are stripped of direct identifying information- names, addresses and identifying number but may contain zip codes or dates of treatment. Research involving only a limited data set may not fall under IRB oversight/meet the definition of human subject but falls under HIPAA requirements.

IRB Data Security Guidance

Example	Data Class (1-4)	Approved Practices	Prohibited Practices	Comments
		SFTP, SSH, SMB 3). Cannot transmit via email unless encrypted and secured with a digital signature.	not authorized in the DUA.	
Personally identifiable information (PII) for research. Video recordings or photos with faces Identifiable interview and/or survey information Education records	3	Storage on an ITS secured server. Storage on workstation or mobile with full-disk Encryption. Transmission: Encryption required (e.g., TLS or HTTPS or secure file transfer protocols, SFTP, SSH, SMB 3). Cannot transmit via email unless encrypted and secured with a digital signature.	Storage on USB drive or cd unless encrypted. E-mail of data files. Use by a person or for a purpose not authorized.	Research Data is Class 3. Recordings, not publically obtained.

IRB Data Security Guidance

Example	Data Class (1-4)	Approved Practices	Prohibited Practices	Comments
Health Data including identifiers	4	Two-step verification required for access. Logs of access to data or physical access to location.	Storage on USB drive or cd unless encrypted. E-mail of data files. Use by a person or for a purpose not authorized in the DUA.	HIPAA Private Health Information (PHI) requires a specific HIPAA authorization, unless an alteration or a waiver of authorization has been approved.
Data obtained during a study that was deemed “not human subjects research”	3	Storage on an ITS secured server. Storage on workstation or mobile with full-disk Encryption. Transmission: Encryption required (e.g., TLS or HTTPS or secure file transfer protocols, SFTP, SSH, SMB 3). Cannot transmit via email unless encrypted and secured with a digital signature.	Storage on USB drive or cd unless encrypted. E-mail of data files. Use by a person or for a purpose not authorized.	Data security is still governed by NAU policy, but not through the IRB.
Biometric information /	3	Storage on an ITS	Storage on USB drive or cd	Biometric information

IRB Data Security Guidance

Example	Data Class (1-4)	Approved Practices	Prohibited Practices	Comments
human subjects data with identifiers or a code key of identifiers	Minimum class 3, depending upon the type of data that is obtained, it could become a level 4 and would need to have more protections in place.	secured server. Storage on workstation or mobile with full-disk Encryption. Transmission: Encryption required (e.g., TLS or HTTPS or secure file transfer protocols, SFTP, SSH, SMB 3). Cannot transmit via email unless encrypted and secured with a digital signature.	unless encrypted. E-mail of data files. Use by a person or for a purpose not authorized in the DUA.	includes finger or voice prints and human DNA profiles. Other biometric data *may* be considered human subjects research depending on the ability to identify individuals.
Research with identifiable biospecimens	3 Minimum class 3, depending upon the type of data that is obtained, it could become a level 4 and would need to have more	Storage on an ITS secured server. Storage on workstation or mobile with full-disk Encryption. Transmission: Encryption required (e.g., TLS or HTTPS or	Storage on USB drive or cd unless encrypted. E-mail of data files. Use by a person or for a purpose not authorized in the DUA.	Research Data is Class 3. De-identified DNA or Biospecimens are not human subjects research, **but** the new Common Rule changes require re-evaluation of whether biospecimens can be re-identified with newer technologies/techn

Example	Data Class (1-4)	Approved Practices	Prohibited Practices	Comments
	protections in place.	secure file transfer protocols, SFTP, SSH, SMB 3). Cannot transmit via email unless encrypted and secured with a digital signature.		iques. We expect guidance on the meaning of “identifiable” to change in the next few years.

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. Investigator assessment of the adequacy of the administrative, physical and technical protections should include consideration of the sensitivity of the data in line with the Data Classification and Handling Policy.

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 out 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 in 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 location that is separate from the study data itself.

IRB Data Security Guidance

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.

In reference to storage of unpublished research data, the NAU Data Handling Protocols allow for research data to be stored on a workstation or laptop if full-disk encryption is used or it can be stored on a NAU CIO approved secure server. The secured server does not have to be encrypted. That is, storage and use on an ITS approved share is fine if it is not encrypted since it is located in a secure location. If unsure, researchers need to submit a service-now ticket request to ITS for appropriate data security provisions.

Personally identifiable information (e.g., IP addresses, PHI) must be kept separate from the data. 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. Any requirements of study sponsors shall not be construed to require less security than indicated in this guidance or any other University data management policy.

Security Provisions

Human Research records require varying levels of security depending on the level of risk, type of information collected, and the level of consent obtained from subjects. Investigators must use NAU data handling protocols when storing research data.

HRPP 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.
- Using a NAU CIO approved secure server
- For Macintosh users, install the latest updates at: https://support.apple.com
- For Microsoft Windows users, install the latest updates at www.windowsupdate.com.

Encryption

IRB Data Security Guidance

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, if encryption is needed, it is recommended that the highest level of data encryption be used, within the limits of availability and feasibility.

Researchers handling sensitive data on laptops or workstation should consult the NIH Guide to Storage on End User Devices.

Specific Examples of Data Security and Encryption at NAU			
Example	**Data Class**	**Compliant Solution**	**Comments**
Collection of PII/PHI though a REDCap survey	3	Jefferson REDCap Server	
Data Analysis of class 3 survey data	3	Adams Analysis server	
Analysis of de-identified survey data from above	1	Any University computer IT system	As long as it is not combined with data that could allow re-identification.
Collection of data containing health information but not any identifiers under HIPAA.	1	Jan redcap server	Jan, although not as secure as Jefferson, has a REDCap available for non-sensitive data surveys.
Limited Data Set from an external partner	3	Analysis on Monsoon cluster	Although Monsoon is not *encrypted,* it is *secure* (approved as secure by the CIO)
	3	Analysis on dedicated workstation that has full disk encryption and multifactor authentication enabled	Researchers should also use secure methods to move the data onto and off of the workstation

Use of external vendors for data storage and transfer (i.e., cloud storage) is permitted subject to following NAU ITS security guidelines. For highly sensitive data such as studies determined to be more than minimal risk to participants or that involve Protected

Health Information (PHI) subject to HIPAA regulation, must be protected with the highest levels of security that are reasonably attainable. For example, the data must be encrypted, stored on secure servers, using encryption 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. Researchers are responsible for understanding and adhering to data owner/data system requirements and for communicating data restrictions to the IRB.

Project Closure and Record Retention

Approved human subject research projects may be closed at the time all data have been collected. Data for which no identifying key exists can be kept for further analysis and do not require continuing review and approval by the 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:

a) The length of time required by law; or
b) As long as the sponsor requires (for sponsored research); or
c) 5 years after the completion of the research; or
d) 5 years after the age of majority, if the research involves children; or
e) Unless another time period is specified by regulation, policy, or agreement

For accessibility purposes (such as audit), original, signed consent forms must be kept in a secure location on Northern Arizona University property. Store research records as described in the IRB approved project and following the Data Classification and Handling Policy.

Should a researcher leave the University, NAU and researcher should come to agreement over whether the researcher may take the original data or an identical copy of the data. If the researcher takes the original data, a copy must be left at NAU. In addition, the researcher must agree to retain the original data for the required retention period and to provide access to the original data to the institution as well as other individuals or entities having a legitimate need for access.

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.

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.