**Guidance and Procedures for Investigators**

**Topic: Data Storage and Security Recommended Language**

The following IRB recommended language can be incorporated into the protocol synopsis. NOTE: Where appropriate, and as needed, the content/recommended language should be adjusted for, or tailored to, each IRB submission/project.

**Procedures**

“Research data, in hard copy or electronic form (CDs, DVDs, digital or magnetic tape/files, hard‐drives, flash‐memory drives, recordings, etc.) will be stored and managed in a secure manner following federal, state, institutional and sponsor (if applicable) policies, practices and guidelines. Further, research documents including electronic documents containing subject data, identifiers and linked data will be securely stored (locked file cabinets, lockers, drawers; password-protected file server, software system; etc.) in accordance with standard document management practices. At all times, only listed key personnel specifically designated and authorized by the Principal Investigator shall have access to any research related documents. All such personnel will be properly trained and supervised regarding the management and handling of confidential materials. The Principal Investigator assumes full responsibility for such training, supervision, and conduct. Any identifiers (if collected and retained) will not be published and will be removed, destroyed or stripped from the research data upon study closure.”

**Other Guidance Items/Points to Consider**

* The Principal Investigator shall maintain all documentation (hard copy or electronic form) relating to research once the study is complete. This includes portable data storage devices such as flash drives. Refer to section 7.6 “Record Keeping Requirements for Investigators” in the North Texas Regional IRB Policies and Procedures Manual for record retention requirements.
* Co-mingling of personal data with research data, including research-generated protected health information, creates opportunities for breach of confidentiality by allowing access to research data by non-research personnel. Therefore, personal computers, devices or flash drives containing personal data, or information should NOT be used to store research data at any time during the study. Instead, a dedicated research-only, or work-issued device (computer, flash drive, etc.) designated for research data should be used to collect and store research data.
* HIPAA Component: When collecting, using, analyzing and/or storing identifiable health information (protected health information), please ensure that the data collection platform/medium (e.g., survey tool, Zoom) and storage system being used meets HIPAA compliance requirements. This information should be discussed in the protocol. Contact your institution’s relevant information security official for guidance on authorized/permissible HIPAA-compliant tools/devices. Where applicable, or appropriate, provide supplemental information (if any) regarding any third-party software tool (e.g. salesforce).
	+ For UNTHSC: [Approved Services Decision Matrix - Information Technology Services (unthsc.edu)](https://www.unthsc.edu/Information-technology-services/approved-services-decision-matrix/)
* **Audio-recordings**: Ensure the protocol appropriately addresses the storage, transcription and destruction of the recordings (e.g., where they will be stored, who will transcribe and destroy recordings, etc.). If transcription services will be used, please provide information about this topic in the protocol synopsis.
	+ For example: “Transcription agency personnel will follow the agency’s standard policies and procedures for data security. Data are inaccessible to other customers and the public and the professional transcription agency provides continuous training for their staff on best practices for security and privacy.”