Data Security Guidance for Human Subject Research

Federal regulations require the Wright State University IRB to determine the suitability of security measures utilized by the researcher for the protection of privacy of subjects and the confidentiality of the research data. People who volunteer to participate as subjects in research do so with the understanding that the researcher(s) will protect their identity and the information obtained about them. These guidelines attempt to outline the basic data security provisions expected from researchers during collection, transmission, and storage of data.

Please note this guidance is for Wright State University researchers. Premier and VA Medical Center researchers will need to comply with their respective data security policies.

If your study is funded, please refer to your funding agency's data security guidance requirements.

- General Guidelines
  - Only collect the minimum necessary subject identifiers as required for the research.
  - Remove subject identifiers from data files whenever possible.
  - Coded data files stored electronically must, at a minimum, be password protected using a strong password/passphrase.
    - Data/specimens must be labeled with a code or number in such a manner which de-identifies the data/specimen; initials are not permitted and must not be part of the code.
  - The master code key for coded data should be stored in a separate location from the coded data. This key should be encrypted.
  - Remove/destroy subject identifiers as soon as they are no longer needed.
  - If subject identifiers will be retained in the data files because of the specific needs of the study, additional justification must be provided by the researcher in the IRB application.
  - If identifiable sensitive data are stored electronically the files or device must be encrypted.
  - If the study qualifies, researchers should obtain a certificate of confidentiality if the data is high-risk.
  - Studies that are not restricted to US participants and include European Union participants may need to comply with General Data Protection Regulation (GDPR).
- Audio and Video Recordings
  - Researchers should be mindful of confidentiality as it pertains to the recording medium (e.g., SD/micro-SD card, iPhone, audio recorder, etc.) they are using for storing recordings.
  - Researchers should ensure the audio and video recordings, once no longer needed, are securely erased from the recording device.
  - Based upon the risk level of the data, additional security measures should be taken to ensure the recordings are not backed up to a local computer, cloud service, or third-party vendor.
  - For high-risk studies, if the unencrypted audio and/or video recordings will be retained longer than a week the researcher should utilize voice changing technology and/or pixilate faces on the video recordings.
- Audio and Video Recording Transcription Service
  - Transcriptions services must have a confidentiality agreement in place as part of their service.

- Web forms and survey providers
    - Wright State University has obtained licenses for use of Qualtrics and REDCap survey software. Use of other survey providers (Survey Monkey, Survey Gizmo, Google Forms, etc.) is permitted for minimal-risk studies that do not collect identifiable data.
    - Researchers should be cautious about stored IP addresses and data that could potentially be accessed by a third-party.
    - If IP addresses are collected, they should be removed from the dataset as soon as possible.
    - Web forms and surveys should use secure protocols (https) with a minimum key length of 128-bits for transmission during the collection of information via the web and the server(s) used in the collection and storage of the information should encrypt the data as it is collected and stored. It is recommended to use data collection platforms that utilize these protections.
    - Ensure you carefully review the site's data security policy. If the site collects and/or stores identifiable information and/or links survey responses to individual participants, you must make this clear within your IRB protocol and within the informed consent document(s).
    - Researchers conducting web-based research should be careful not to make guarantees of confidentiality or anonymity, as the security of online transmissions is not guaranteed. A statement in the informed consent form indicating the limits to confidentiality is required. The following statement may be used: "Your confidentiality will be maintained to the degree permitted by the technology used. Specifically, no guarantees can be made regarding the interception of data sent via the Internet by any third parties."
    - For internet-based surveys, include "I agree" or "I do not agree" buttons on the website for participants to click to indicate their active choice of whether or not they consent to participate. They must be formatted in a way that will allow participants to skip questions if they wish or provide a response such as "I choose not to answer." Also, at the end of the survey, there should be two buttons: one to allow participants to discard the data and the other to submit it for inclusion in the study.
- Cloud-based Storage
    - Datasets may be stored online (e.g., cloud-based solution) depending upon the risk-level.
        - Important considerations for datasets stored online include:
            - Data storage geographical location
            - Backup and retention policy
            - Deletion policy
            - Rights the cloud provider claims for the data
            - Isolation guarantees that the provider offers

Service:	No Identifiers	Identifiable Not Sensitive	Identifiable Sensitive	FERPA Protected	HIPAA Protected
WSU OneDrive	X	X			
Dropbox Personal	X	X			
Dropbox for Business Standard or higher	X	X	X	X	X
IDrive Personal	X	X			
IDrive Team/Business	X	X	X	X	X
Google Drive	X				
Survey Monkey	X	X			
Survey Gizmo	X	X			
REDCap	X	X	X	X	X
Qualtrics	X	X	X	X	X
Proofpoint Secure Share	X	X	X	X	X

- Social Media
    - Open groups and pages on social media can be utilized for low risk studies which contain public information and discussions.
    - Social media used for recruitment should utilize a closed group for sensitive discussion. As a reference, Facebook has published information regarding their privacy settings for groups.
    - At the conclusion of the study the social media group/page should be deleted to ensure that the information is no longer accessible.
- Mobile Devices
    - Researchers must be mindful of the mobile devices (e.g., iPhone, iPad, tablet, etc.) used in the collection of information from participants and ensure that the data is kept secure at all times including the collection, transportation, usage, and disposal of the information collected.
    - The settings on these devices should disable cloud back-ups.
- Special Population Guidelines : Children
    - The Children's Online Privacy Protection Act (COPPA), enacted by the Federal Trade Commission applies to the online collection of personal information from children under the age of 13 and is intended to protect children's privacy and safety online. Additionally, COPPA is intended to place parents in control over what information is collected from their children online. COPPA requires websites to display a privacy policy, obtain verifiable parental consent, and disclose how the information will be used. If you need to collect data online from children, it is important to review COPPA regulations and maintain compliance.
- Physical controls
    - Physical keys/swipe cards used to access offices, desk drawers, cabinets, a locked safe, etc. should only be in the possession of those listed on the IRB application and approved for access.
    - Entrance Keypad/PIN #'s should be reset if compromised, lost, or stolen.
    - Limit physical and electronic access to any area, office space, computer, or device containing subject identifiers.
    - Never leave physical media/hard-copy data unattended on a desk, printer, fax machine, copier, etc.
    - Never take identifiable information home with you.
    - Never leave identifiable information in a vehicle.
    - Be aware of your surroundings when processing or discussing identifiable information in order to protect against "shoulder surfing" and eavesdropping.
    - The computer monitor used for viewing the data must be positioned away from any windows or anyone passing by.
- Document security
    - When protecting data by password-protecting the document, create strong passwords.
- Mobile apps and Devices
    - Avoid storing subject identifiers or Personal Health Information (PHI) on portable devices (e.g., laptop computers, digital cameras, portable hard drives, thumb/flash drives, USB memory sticks, iPads, etc.) as these devices are particularly susceptible to loss or theft.
    - If there is a necessity to use portable devices for initial collection of sensitive data with subject identifiers, the data files or devices must be encrypted, and data files or devices must be transferred to a secure system (e.g., server behind firewall) as soon as possible.
    - Portable devices must be sanitized once they are no longer required for the project.
    - Avoid Mobile Apps which automatically upload content to third-party sites. If you choose to utilize a mobile app, seek expert IT security review of the app by the CaTS.
    - The researcher is responsible for disclosing potential risks associated with downloaded mobile apps. Additionally, the researcher has the responsibility to understand known and

potential risks regarding the app and convey them to the participant (CFR 46.116). Typically, commercial apps publish a "terms of service" which detail how app data will be used by the vendor and/or potentially shared with third-parties. The researcher must understand these terms and convey them to the participants; as well as monitor the terms for any updates from the vendor.

- Transmission
  - Use only secure modes of transmission of data; identifiable data or PHI must be encrypted.
- Off-Campus Storage
  - If storing de-identified data off of the Wright State campus, the electronic storage devices must, at a minimum, be password protected.
  - If data is sensitive and identifiable or is PHI, it must be encrypted.
  - Hard copy data must also be kept secure (locked file in a locked home office). Hard drive or mobile devices should also be stored in this manner until such time that the data can be removed from the portable device.
- Retention
  - Information in either an electronic or physical format, once no longer required, should be considered for destruction or sanitization; and must adhere to appropriate data retention policies.
- External Hard Disk and USB Drives
  - External hard disks and USB drives can be used for storing de-identified data.
  - Files and/or directories on an external hard disks/USB drives should be password protected.
  - External hard disks and USB drives should be encrypted, with the encryption key kept in a secure location and only known by the researcher and those deemed necessary that are listed on the approved IRB study. Identifiable data should not be stored on USB drives.
  - External hard disks and USB drives should be stored in a secure location restricted to only those listed on the approved IRB study.
  - Transportation of external hard disks and USB drives should be restricted to only those listed on the approved IRB study.
  - Once the information is no longer needed the hard disk/USB drive must be sanitized in order to protect the confidentiality of the data. Once the hard disk/USB drive has been sanitized the device can be repurposed.
  - If the hard drive/USB drive becomes inoperable and is not repairable the device must be destroyed in order to protect the confidentiality of the data.
  - Contact the Wright State IRB for guidance if you need to use hard disk/USB drive to store identifiable information on a short-term basis (i.e. transferring data to new University).
- CD's and DVD's
  - While not ideal, identifiable human subject research data can be stored on CD's or DVD's, however, encryption must be used.
- Email
  - Identifiable human subject research data must not be emailed.
- Backup's
  - Backups should be encrypted during transmission to the backup system and should remain in an encrypted format. The backup should be stored in a secure location separate from the original data.
- Breach of Confidentiality
  - The PI must report any inadvertent breach of confidentiality of the research data which causes harm or places subjects or others at a greater risk of harm (including physical, psychological, economic, or social harm) to the IRB within 5 calendar days of the researcher becoming aware of the event.

- Media Sanitization
    - Ensuring the confidentiality of information requires that all physical media (CDs, DVDs, hard drives, etc.) be disposed of properly. This means that, in addition to being properly erased before being discarded, hard drives must also be erased before being returned for any type of warranty work. Additionally, other media such as CDs, DVDs, and paper must also be carefully destroyed if they contain Protected information. CDs and DVDs should be broken into multiple pieces, and paper documents should be shredded.
- General Computing Recommendations
    - Desktop Computers/Servers
        - Non-networked computers can be used for storage of data; however, it should be password protected and it is strongly recommended to encrypt the hard disk.
        - Operating system is current with updates and security patches.
        - Applications are current with updates and security patches.
        - An antivirus/malware software application must be installed and up to date.
        - Accounts on the computer/server are unique and password protected with strong passwords/pass-phrases.
        - Guest accounts are disabled.
        - Regular auditing of user accounts which have access to data.
        - Restrict physical access to the computer/server.
        - Ensure that your session is locked when you step away from the computer.
        - Applications and services installed will operate in a non-administrative mode.
        - A mechanism should be in place to block access to idle sessions (e.g., screensaver or application timeout).
        - Employ a mechanism to hinder an attacker from guessing passwords (e.g., account lockout after a set amount of bad password guesses).
        - Device must use an operating system that is supported to receive new security updates. Many devices use older operating systems, such as Windows XP, Windows 7, MacOS Maverick, etc. This software is no longer supported by the vender, are not secure, and should not be used as part of research.
    - Smartphones, tablets, and other mobile devices
        - Update mobile device operating system on a regular basis.
        - Do not use older devices that are no longer supported by the vender.
        - Applications are current with updates and security patches.
        - Configure mobile device auto-lock and require a password/passcode for reentry.
        - Researchers should consider setting the mobile device to erase data after 10 failed password/passcode attempts.
        - Only connect to secure Wi-Fi networks.
        - Disable Bluetooth when not in use.
        - Delete all information stored on a mobile device prior to disposal.
- Wright State IT Guidelines and Additional Resources
    - Wright State IT Security Policy
    - Wright State Data Classification and Risk Matrix
    - Wright State Security Training
        - Introduction to Computer Security
        - HIPAA Security Awareness
        - Data Encryption: How Do I Protect Sensitive Information?
        - REDCap
        - Do IT Wright: Six Quick Strategies for IT Security
        - Do IT Wright: Data Security Video Training
        - Do IT Wright: Smart Phone & Cloud Storage Security Video Training