Best practices around collecting, reviewing, organizing, and analyzing human subjects information and data must be observed when working remotely. The primary goal is to ensure that you are protecting subject privacy and confidentiality through effective management of your electronic and physical environment and use of sound data security measures.

**MANAGING YOUR ELECTRONIC AND PHYSICAL ENVIRONMENT**

1. As much as possible, identify and set-up a workspace in an area over which you can control access and store records and data securely. Shut your door to help ensure privacy and confidentiality of records and data.

   If you must work in an open area, or if you share a defined workspace, ensure that you take steps to:
   - Conduct videoconferencing in private using secure settings; wear headphones to limit what others who may be nearby can hear of your discussion; be alert to what appears in your background.
   - Position or block your computer screen such that others cannot see subject information or data; close your laptop or lock the screen when you are away from it.
   - If possible, close doors or screen off your work area to further ensure privacy and confidentiality.

2. During your work day, ensure that if you must leave the workspace, and there is a possibility that others could access the space, that you gather and store research records and subject data before stepping away from the area.

3. At the end of your work period, gather and store away research records and subject data so that others cannot access the materials.

4. If using non-U-M computers or other devices, ensure that you:
   - Have correctly configured the items to meet U-M security standards.
   - Are using devices to which others will not have access, or if you must share, do not store subject information or data in files and folders that are accessible to others; follow appropriate encryption guidelines or only store the information or data on secured external drives.
   - Store U-M data in approved storage locations.
   - Cover your computer webcam when not in use.

5. Use secure connections. Use the U-M VPN when connecting from off-campus. **NOTE:** MiWorkspace Windows computers are equipped with an “always on” VPN-like client called DirectAccess; no need to use the U-M VPN.
DATA SECURITY

Manage your data security consistent with what you have described in your IRB research application for the project. General best practices for data security include:

1. Details on what tools can be used for which institutional data types can be found in the Sensitive Data Guide. This includes cloud computing & encryption standards.

2. All data collection and storage devices must be password protected with a strong password. A strong password requires a level of complexity. Create a unique password for just U-M use. Don’t share your password with anyone (including RAs, colleagues, or family members).

3. All sensitive research information on portable devices must be encrypted.

4. Access to identifiable data should be limited to only those individuals with a reason to have such access and never with anyone outside of the study team. Track access to shared folders (e.g., M+Box) and remove individuals no longer with the project.

5. Identifiers, data, and keys should be placed in separate, password protected/encrypted files and each file should be stored in a different secure location.

6. If it is necessary to use portable devices for initial collection of identifiers, the data files should be encrypted and the identifiers moved to a secure system as soon as possible. The portable device(s) should be locked up in a secure location when it is not in use. All data collected on portable devices should be transferred to an approved service as soon as possible after collection, and deleted from the portable collection devices.

7. The PI should consult with their departmental IT Security Liaison to discuss how to correctly configure desktop computers, laptops, and other external devices for safe use in the collection and storage of research data when working remotely.

8. U-M +Google Mail and Calendar services may not be used to collect, store, or transmit sensitive human subjects research data or protected health information (PHI). The Sensitive Data Guide provides information on what specific IT resources may be used with sensitive human subjects research data and protected health information.

9. If utilizing any cloud-computing services, the PI must follow the U-M safecomputing guidelines.

10. If research includes sensitive identifiable data, outside consultants or vendors should be required to sign a confidentiality agreement.

11. If the research design requires or allows, the PI should delete or destroy identifiable information as soon as possible after collection.

If you have any questions about these guidelines and your management plan, please contact your project PI/supervisor. If you have any challenges in creating privacy conditions in your work environment, please reach out to your project PI/supervisor to discuss options for completing the project work. You may also reach out to your IRB liaison at irbhsbs@umich.edu or by calling 734-936-0933.
RESOURCES

IRB-HSBS Data Security Guidelines
https://research-compliance.umich.edu/data-security-guidelines

U-M Safecomputing
https://safecomputing.umich.edu/protect-yourself/be-safe-online/working-remotely

Security Unit Liaison Listing
https://safecomputing.umich.edu/it-security-professionals/security-unit-liaisons/directory

ADDITIONAL RESOURCES

Secure Your Computer, Smartphone, and More
- Secure Your Devices
- Video: Secure Your Devices: For You and the U
- Your Responsibilities for Protecting Sensitive Data When Using Your Own Devices
- Antivirus for Personal Computers
- Encrypt Your Data and Devices
- MiWorkspace Security & Privacy

Secure Your Connections
- Secure Your Internet Connection (includes VPN info for all U-M campuses)
- Secure Your Home Wireless Network

Protect Sensitive Data
- Sensitive U-M Data on Personal Devices
- Protect Sensitive Data
- Comply With Laws, Policies, and Regulations

Protect Your Privacy
- Basics: Protect Your Privacy
- U-M and Privacy
- Choose Privacy on the Web
- Instructions to set Zoom virtual background to hide your surroundings
- Privacy and Videoconferencing
  - Secure Meetings in BlueJeans
  - How to Secure a Hangouts Meet Session
  - How to Secure Meetings in Zoom