Working Remotely with Human Subjects Research: Privacy and Confidentiality Considerations

Purpose:

The information in this guidance outlines privacy and confidentiality considerations for working remotely (e.g., at home, telecommuting, when traveling, etc.) on human subjects research.

In this Document:

Preparing to work remotely
Working remotely
Additional Information

Preparing to work remotely:

- Develop a communication plan for the research team. Ensure personnel know whom to contact if problems or concerns arise.
- Verify that research personnel have resources and information necessary to carry out protocol activities and ensure privacy and confidentiality.
- Establish research team policy and guidance related to privacy, confidentiality, and data security. Research team specific policy may include instituting confidentiality agreements, logs to check out/in physical files, creating guidance in case of a confidentiality breach, etc.
- Confirm that data/records/equipment/supplies are permitted to be taken/accessed off-campus.
- Remove identifiers from data (anonymize) or create subsets of de-identified data with which to work remotely.
- Ensure that remote access to electronic data files meets the appropriate level of IT's Minimum Security Standards (e.g., data storage on CyBox, encrypted portable storage).
  - Researchers are reminded that FERPA or HIPAA protected data are subject to additional safeguards and restrictions.
- Download and install any necessary software while on campus (e.g., Cisco AnyConnect for VPN, Okta Dashboard, Webex Meetings).
Reminder: Researchers are obliged to follow the privacy and confidentiality protections specified to participants as part of informed consent.

Researchers must also follow the privacy and confidentiality protections outlined in the approved IRB protocol. In general, applications approved through IRBManager have some degree of flexibility, as researchers are asked to agree to follow ITS Minimum Security Standards, as opposed to identifying specific data security methods. HOWEVER, researchers may have noted more specific security provisions which they are obliged to follow.

If remote work requires changes to the approved protocol, informed consent forms, or other materials submit an Amendment for Modification through IRBManager.

Working remotely:

Electronic data/records considerations

- Data must be stored according to ITS Minimum Security Standards (i.e., encryption, CyBox).
- Work within Okta cloud platforms¹ using iastate.edu credentials and do not store data copies locally.

Some programs (e.g., SPSS) are not currently available through Okta. If data are temporarily downloaded for analysis, care should be taken to ensure all local copies of the data are securely removed/deleted once analysis is complete.

- Avoid working on shared computers/devices if possible.
- Avoid public Wi-Fi.
- Use strong passwords for home networks and devices.
- Share or access data via CyBox, Remote Desktop, Okta cloud platforms, etc. Do not send data sets via email.

Identified or sensitive paper records/documents/questionnaires/log considerations

- Keep in a secure location when not in immediate use.
- Flip-over or cover identifiers when stepping away temporarily.
- Use locked storage when possible.
- Stay organized and know what physical information is in your possession.
- Research labs may choose to implement a log in/out process for physical records/materials.

¹ ITS approved Cloud platforms are available in the Okta Application Dashboard, accessible from the ISU Sign On page.
Data collection activities

- When conducting interviews via phone/videoconferencing – take precautions to protect participant privacy (e.g., do not conduct a video interview in a common room where roommates/family members may overhear).
- Separate participant contact/identifier information from data, or link indirectly via codes and a key. Store the key linking identifiers and data in a secure location separate from the data.
- Inform roommates/family members of confidentiality expectations.
- Do not video/audio record data collection activities unless approved by the IRB.
  
  This changes the IRB’s data security/confidentiality assessment. Such a change may not be implemented without prior approval or confirmation of exempt determination by the IRB office. This applies to both Exempt and Non-exempt human subjects research.
- Ensure any necessary safety precautions can be followed in a remote site (e.g., spotters to prevent falls, safety equipment is available and functional, etc.).

Additional Information

“Working Remotely” Iowa State University Information Technology https://www.it.iastate.edu/remotework

Document History

<table>
<thead>
<tr>
<th>Created:</th>
<th>3/11/2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated:</td>
<td>3/13/2020</td>
</tr>
</tbody>
</table>