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. While remote technologies can be a useful resource, there are unique considerations related to protecting participant privacy and confidentiality.

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 ITS 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).
- Use only ISU-supported tools. 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: https://web.iastate.edu/signons
Data collection activities

- Work within Okta cloud platforms using iastate.edu credentials when selecting data collection platforms. Use only platforms supported by ISU.

- Inform participants of steps they can take to protect privacy (e.g., closing their web browser after survey completion, avoid using shared devices, finding a private location to complete interviews, etc.).

- Be familiar with platform settings necessary to protect privacy. Whenever possible, disable functions that automatically collect electronic identifiers, such as IP addresses or cookies.

- When conducting interviews via phone/videoconferencing – take precautions to protect participant privacy (e.g., do not conduct a video interview in a publicly occupied space or a common room where roommates/family members may overhear).

- Focus groups conducted using videoconferencing software (i.e. Webex or Zoom) must include extra precautions as confidentiality and privacy of all group participants relies on other members.
  - Group members should be reminded that they are each responsible for taking precautions to protect the privacy of fellow participants.
  - Researchers should configure videoconferencing software to prohibit recording by participants.
  - Participants should be instructed to not record/take screenshots
  - Participants should be mindful about location to prevent roommates/family members/public from easily overhearing/seeing other participants. Use a private location and be conscious of public areas, shared common areas, poor acoustics, etc.
  - All participants should be reminded of the unique limitations to privacy on digital platforms and to use discretion when sharing.

- 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.

- Do not video/audio record any data collection activities unless approved by the IRB.

  Creating audio/video recordings 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.).

- Use of Mturk, or similar crowdsource platforms, introduces additional privacy and confidentiality concerns as data collection cannot be anonymous. Identifiers (e.g., worker IDs) are necessarily collected. Data collected via Mturk or similar platforms is not considered anonymous.
  - Inform participants that their responses are not anonymous and how identifiers will be handled to protect privacy (e.g., timely separation of worker ID from responses, etc.).
Collect data outside of the crowdsourcing platform, such as via Qualtrics, to ensure data are not accessible by the platform.

Additional Information

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

“Modifications to Exempt Research” Iowa State University Office for Responsible Research [https://www.compliance.iastate.edu/sites/default/files/imported/irb/guide/docs/exempt-research-modifications.pdf](https://www.compliance.iastate.edu/sites/default/files/imported/irb/guide/docs/exempt-research-modifications.pdf)

Document History

<table>
<thead>
<tr>
<th>Created:</th>
<th>3/11/2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3/13/2020</td>
</tr>
<tr>
<td></td>
<td>3/19/2020</td>
</tr>
<tr>
<td></td>
<td>3/20/2020</td>
</tr>
</tbody>
</table>