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:

- Develop a communication plan for the research team. Ensure personnel know whom to contact if problems or concerns arise.
- Verify that research personnel have the 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).

Important:

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. Note that research data are classified as moderate or higher.
- Use Iowa State IT Security approved digital tools (e.g. software, apps, programs).
    - All digital tools should be accessed using **iastate.edu** credentials. Researchers must not use private non-ISU accounts to conduct research, unless granted an exception by IT Security.
    - Work within Okta cloud platforms whenever possible.
- Do not store data copies locally on devices not managed by Iowa State.
- Avoid working on shared computers/devices.
- Avoid public Wi-Fi or networks that are not password protected.
- 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.
- Lock your computer when stepping away.
- Ensure that software updates are up to date.

IT Security maintains a list of Approved Vendors. Digital tools not available through Okta and not on the list must be evaluated by IT Security if they have a cloud component that effectively allows access to data by a third party (i.e. the software vendor).

Stand-alone software apps that do not have a cloud component can be used without IT Security approval, but must be used in compliance with the Terms of Service for that tool.

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.

Data collection activities

- Use IT Security approved technology tools accessed using iastate.edu log-on credentials.
    - Digital tools not available through Okta and not on the IT Security Approved Vendor list must be evaluated by IT Security if they have a cloud component (effectively allows access to data by a third party (i.e. the software vendor)).
- 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 the 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.
- Avoid publicly posting videoconferencing links to prevent unauthorized persons from accessing the virtual space.
- 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. In general, 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 crowdsource platform, such as via Qualtrics, to ensure data are not accessible by the platform.

Additional Information

Approved Software and Vendors | *Iowa State University Information Technology*

Securing Your Devices |*Iowa State University Information Technology*

Learning and Working Remotely| *Iowa State University Information Technology*

Modifications to Exempt Research | *Iowa State University Office for Research Ethics*

Mechanical Turk | *Iowa State University Office for Research Ethics*

Document History

Created/Approved: 3/11/2020
Updated: 3/13/2020
3/29/2020
3/20/2020
10/20/2020
1/17/2024