Guidance for Human Subject Research (HSR) regarding moving in-person research activities to online or remote activities due to the need for social distancing in response to COVID-19

*Below is guidance from the CMU Institutional Review Board (IRB) Office and the CMU Information Security Office (ISO). Note that this is general guidance and may not be applicable to every situation. As always, please contact the office directly with specific questions.*

---

**IRB:**

If, consistent with recommended social distancing practices, you need to move interactions with research participants from in-person to online, first check your CMU IRB-approved protocol. If you need to make changes to the protocol to account for changes in practice, please submit a modification through SPARCS IRB. We recommend adding new procedures, not removing any of the existing procedures, to accommodate this change. This way, the protocol still addresses procedures done previously and will allow you revert back to in-person procedures at a later date without submitting another modification. When reading through your currently approved protocol to see where modifications are needed, remember to check all sections, as modifications may be needed in more than the study scope. Also remember to check your consent forms, consent scripts, recruitment materials, etc. Thoroughly checking all of your submission materials and making modifications to all applicable sections will allow the IRB to process the review more quickly. Delays may occur if incomplete modification requests are submitted and the IRB has to send them back for corrections.

The IRB will prioritize these reviews. Once you have submitted the modification in SPARCS IRB, email the IRB mailbox at irb-review@andrew.cmu.edu to alert the IRB that you are requesting prioritization of the review of your modification. Please also use this email if you have any questions or would like assistance.

**ISO:**

WARNING: While this guidance applies to most HSR conducted under a CMU IRB approved protocol, you may be working with data that has other security requirements. If this guidance conflicts with a data use agreement or other type of agreement, you must follow the agreement. For other options, contact ISO (iso@andrew.cmu.edu).

The ideal option for accessing research data remotely, is to use the General Campus VPN (https://www.cmu.edu/computing/services/endpoint/network-access/vpn/index.html) and remote access to the machines/servers that are already storing the data (whether that’s SSH for Linux or Remote Desktop for Windows). That way, the data remains ‘on campus’, protected the same way it’s protected currently, and accessible only to those who should have access to the data.
Some data may be able to be shared via Box or GDrive for viewing by students/researchers. However, Box/Gdrive are 3rd parties, which means that data will be shared with them. That may be problematic, depending on the IRB protocol or data use agreements, where data security requirements may prohibit this.

NEVER save research files on your personal hard drive or personal cloud storage.

Zoom (also a 3rd party) supports end-to-end encryption of conversations for conducting interviews and allows for all data to be encrypted during transmission. It also supports recording of meetings, to be used only when necessary. ISO is currently in discussions with Zoom to determine if recordings in the cloud are encrypted. Local recordings are problematic as they are collected and stored on the local computer.

We strongly recommend that students/researchers:

- are aware of their surroundings (i.e., not accessing sensitive data while at Starbucks, or with curious roommates),
- avoid using shared computers, or if they must, have a separate login for yourself that does not have administrative privileges,
- apply all patches available for your operating system and applications, and
- make sure there is anti-malware software running (where possible).

More information and technical details can be found at
https://www.cmu.edu/computing/support/remote-it-standards.html

If you have questions regarding data security, you can email iso@andrew.cmu.edu for more information.