**THE IRB’S ELECTRONIC AND HARDCOPY DATA REQUIREMENTS**

Please address the questions below which are designed to highlight the security procedures in place to safeguard applicable hardcopy and electronic data. Even for anonymous data, there needs to be evidence that the researcher(s) have done their due diligence to protect the integrity of the data file(s).

1. Explicitly state which **faculty and/or students** will have access to the hardcopies and/or electronic data files that are created/used.
2. If electronic data files are created/used, will the data be **stored** on a network, a local desktop or laptop computer, or an external data storage device (e.g. flash-drive)?
3. If electronic data files are created/used—whether they’re stored on a computer, network, or external data storage device (e.g. flashdrive), access to the files on the computer, network, or external storage device holding the data files must be **password-protected by a security login**.
4. If electronic data files are created/used, who has **access** to the computers and/or data storage devices warehousing the data? This differs from item (a) in that it is specifically inquiring about access to **office(s) or domiciles** that warehouse the computers or external data storage devices that hold the data.
5. All computers used to access and/or store the data file(s) are required to have an **automatic log-out** after five minutes of inactivity? This setting must be activated on the computers to prevent unauthorized access to the data.
6. Will the data be **encrypted**? This is NOT required, but it is recommended for sensitive data with any identifying information.
7. The data file(s) should not be **emailed** from one researcher to another, as this exposes the data file to possible interception from unauthorized parties. Instead, do an internal file transfer instead.
8. If you are using a web-based survey provider such as Qualtrics or Survey Monkey, **IP addresses** CANNOT be collected because this poses a threat to participants’ anonymity and confidentiality.
9. For any instrument or survey **administered online**, participants should be encouraged to do it using their own personal computer, not a public one, to avoid potentially compromised computers that have tracking malware embedded in them that could compromise their identity. Participants should be instructed to avoid leaving a digitally administered instrument/survey open if using a public computer or a computer that others may have access to, as this could also compromise their anonymity. Lastly, participants should be advised to clear their browser cache and page history after completing any digitally administered survey or instrument.
10. **For Zoom-based interviews**: On the scheduled day and time of the interview, participants should log into Zoom using an invitation sent by the researcher(s) that contains the access code that enables the participant to enter the designated Zoom session. The Zoom session should be closed upon the start of the interview to prevent interlopers from potentially accessing the session. Participants should be instructed to change the name on their screen to their chosen pseudonym to protect their identity. If researchers provide participants their phone number in addition to the Zoom link, the IRB strongly recommends that researchers use a Google phone number that routes directly to the researcher’s personal cellphone rather than the researcher’s actual cellphone number. This added measure creates necessary professional boundaries and distancing for safety and security of all parties.
11. Any commercial survey administrators (e.g. Survey Monkey, Qualtrics, et al.) must have industry standard levels of safety, security, and network protections in place. If you plan to use a new or different commercial survey administrator than Survey Monkey or Qualtrics, you will need to obtain a statement of its safety, security, and network protections.