

Tips for thinking about secure data handling and storage when doing research with living human subjects (produced October 25, 2019)

Am I collecting only the data that I need?

Remember, the most secure data are data you never collect in the first place. Go through your research protocol and ask yourself if all the data you plan to collect are necessary to your research.

Best data handling practices:

- Maintain good password practices on all devices (phones and computers); i.e., strong passwords that are stored securely and not reused
- Secure phones used for research data with a numerical code (rather than a fingerprint or face ID) and encryption where possible
- Minimize the number of machines where data are stored
- Remove all data (recordings, typed notes, etc.) off a phone within 24 hours as you collect data
- Make sure you turn off automatic back-up to iCloud/Google Drive on your phone and computer
- Store data to OneDrive (through your Bryn Mawr account) rather than to iCloud or Google Drive; OR, store data on an encrypted personal computer – you can get help turning on full-disk encryption on a college owned computer at the Canaday Help Desk
- Do not store data on a shared or public computer (e.g., in the library), even temporarily
- Access data only via secure wireless connections (not over WiFi in a coffee shop, airport, etc.). Appropriate wireless connections include Eduroam, a well-protected home network, a paid VPN
- Data on any device or hard drive (e.g., phones, computers, tablets, external drives, flash drives, etc.) should not cross international borders, especially when data are of a sensitive nature
- After the research project is finished, ensure secure and complete deletion of data to the extent possible. If data are being stored on OneDrive, please contact the Help Desk to arrange for a secure deletion by someone with admin privileges
- If you are producing hand-written notes, questionnaires, or consent forms, state that you will be storing all paper in a secure location, for example in locked closet, locked box, or locked filing cabinet in your dorm room. Also state that when the research project is finished you will be destroying all hand-written notes, questionnaires, consent forms, etc., using a paper shredder.

How do I communicate my safe data handling practices to the IRB committee?

Great question! You will save yourself and all those reviewing your IRB forms a lot of time if you communicate your data handling strategies effectively and in some detail. This means that you will clearly describe (in a paragraph) what you'll be doing on the IRB forms. For users of "Form B" you can describe your strategies in your answer to question #6 – just keep in mind that that this question asks about both anonymity and confidentiality, so please describe how you'll work to try to ensure both things. For users of "Form C" you will need to thoroughly describe your strategies in your answer to question #7. Also keep in mind that you'll need to clearly communicate these practices to any research participant through the consent form/prompt because they need to know how you seek to protect their information and participation before they can consent to being interviewed or to participate in a survey or questionnaire.

Who may passively or even purposively obtain my research data, and why?

An honest answer to this question is that we can never fully know. Sometimes "leaks" might be accidental and hopefully not of much consequence. Sometimes if other students, other research

Tips for thinking about secure data handling and storage when doing research with living human subjects (produced October 25, 2019)

participants, family members, other members of the community, employers, etc., stumble upon data it could be embarrassing or even worse for your informants. Sometimes, however, certain agents or institutions have an interest in our data, including governments, police, employers, the media, etc. We never really know who may want our data, or how “leaked” data might injure our informants. So, it is best to practice safe data handling procedures from the start and every time we conduct research, even if we feel like our research carries very little risk or will not produce any sensitive data. Our research is extremely important, but it is also extremely important that we work at every step to protect our research participants from any undue or unintended harm or discomfort!