Data Security Inventory

The purpose of this form is to give you and IRB a clear, detailed understanding of what information you will be collecting and how you plan to protect it. When you submit this form, you will receive a copy for your records. We encourage you to submit a copy with your IRB application as well.

* Required

1. Email *

____

2. What is your general research question?

____

____

____

____

____

3. What kinds of data are you gathering? *

____

____

____

____

____

4. What is your plan to protect your data (hard copies or digital) in the period between data collection and data storage? *

5. Will any Personally Identifiable Information be collected? *

This is any type of identifying information (eg ssn, carleton id, phone names, date or place of birth, course numbers, race, age), even if the information does not uniquely identify them.

Mark only one oval.

○ Yes *Skip to question 6*

○ No

De-Identification

The first step is to make sure that you aren't collecting any Personal Identifying Information you do not need.

6. Can you fully de-identify your data? *

See U.S. Department of Health and Human Services standard for de-identification: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard

Mark only one oval.

○ Yes, I am 100% sure and I will explain my process *Skip to question 7*

○ No, my data will require secure processes *Skip to question 8*

○ Not Sure (please contact Paula Lackie for assistance) *Skip to question 8*

De-Identification procedures

See U.S. Dept. of Health and Human Services standard for de-identification: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard

7. How will you be de-identifying your data? *

Include your process for de-identification, where the original data and linking tables will be stored, and for how long.

Highly Sensitive Data

This includes, for example, any information about an individual's educational performance, financial information, present or future health, health care, insurance information, illegal behavior, and/or sexual behavior.

8. Will you collect any health data, or other data that requires extreme protection? (e.g. data on protected groups; children, prisoners) *

Mark only one oval.

○ Yes *Skip to question 9*

○ No

Protecting Your Data

There are several useful sites listed on the IRB data security page. For a useful overview of basic issues, see: Security in a Box (https://securityinabox.org/en/) or Surveillance Self-Defense (https://ssd.eff.org/en/module-categories/basics)

9. Who will have access to your data? *

10. Which devices will have access to your data? *

11. How will you secure digital and physical backups? *

12. Which of these protections against anticipated threats or hazards (during collection, transmission, storage) will you use? *

Check all that apply.

□ Encryption of data on device/s to protect data against loss/theft of device/s
□ Always use Carleton's VPN when off campus and transmit data only after encrypting it
□ Encrypt data in transit regardless of the internet service used
□ Use strong passwords to protect against unauthorized access to any device
□ Store data on a secure Cloud Service accessed only through a Carleton account
□ Maintain all software & hardware updates for all devices that access the data
□ Identifiers, data, and keys will be in separate, password protected/encrypted files and each file should be stored in a different secure locations
□ Assure that all members of the research group understand and use all of these safeguards

□ Other:

13. How long and where will your data be stored? *

14. How and when will data be deleted? *