Boston College Office for Research Protections
Data Storage Policy
Updated: 10.30.2020

ORP has revised its classification system for storing human subjects data to better align with the Boston College Data Security Policy. The BC data policy classifies data among four categories, according to the level of security required. In descending order of sensitivity, these categories are *strictly confidential*, *confidential*, *internal use only*, and *public*. Generally, data collected in IRB-approved protocols falls into the three latter categories.

As the risk posed by the research project increases, so do the requirements for the safe maintenance of human subjects data. If you have questions about IRB requirements for storing and protecting your human subjects data, it is best to contact ORP. The chart below describes how data in IRB approved research projects may be classified.

Terminology from BC Data Security Policy	Public Information	Internal Use Only Information	Confidential Information
What is it?	Information that is generally available to the public, or if it became available to the public, would have no material adverse effect on individual members of the University community or upon the finances, operations, or reputation of Boston College	Information that is less sensitive than confidential information, but that if exposed to unauthorized parties, may have an indirect or possible adverse impact on personal interests, or on the finances, operations, or reputation of Boston College	Information that includes sensitive personal or institutional information. Unauthorized access to this data could adversely affect individuals.
Example	• Names of people who signed up to be contacted about study opportunities • Information publicly posted on websites (staff email addresses, institutional data, etc.)	• Phone numbers, email addresses, and home addresses of study participants • Data that includes identifiers linked to data • Audio recordings that do not contain sensitive information • Completely de-identified survey responses	• Information that has identifiers • Information that is sensitive • Data that you have told participants will be confidential • Information protected by state or federal laws • Information that requires a data security agreement

Where can I store it?	• Departmental Server • Cloud storage platform (Box, Dropbox, Google Drive)	• Departmental Server • RedCap • Linux Cluster	• Departmental Server • RedCap • Linux Cluster

Definitions

- Departmental Servers
  - This is the preferred method of data storage because it is convenient and secure. Please contact your TC or Research Services if you need help getting one set up for your data. Students will need a faculty sponsor to use a departmental server. You can restrict permissions on these folders, indicating people on your research team who should be allowed to access the data. BC backs up these folders multiple times a day.
- REDCap
  - REDCap was originally developed by researchers, for researchers. It was originally developed to function as a data repository, but can be used for data entry, creating surveys, and storing data. PIs can upload data from Excel spreadsheets. BC's installation of REDCap is on a BC-owned server behind the BC firewall. It is backed up regularly.
- Linux Cluster
  - The Linux Cluster can be used for large sets of restricted data that fall under license agreements. It sits behind the BC firewall.

Remember to consider how you have presented your data storage methods in your IRB protocol and in your consent form or other communications with research participants. It is important to be consistent when storing your data according to what has been promised to the participants.