Brandeis
UNIVERSITY
Human Research Protection Program

GUIDE TO DATA MANAGEMENT AND PROTECTION

The risk of harm resulting from a breach of confidentiality varies with the level of sensitivity of the research data. The chart below outlines the risk levels associated with different types of research data, and is followed by options for the management of research data at each risk level.

RISK LEVELS	
Level I	Publicly Available Data Anonymous Data Non-confidential Data De-identified Minimal Risk Confidential Data
Level II	Coded Minimal Risk Confidential Data De-identified Greater than Minimal Risk Confidential Data
Level III	Identifiable Minimal Risk Confidential Data Coded Greater than Minimal Risk Confidential Data De-identified Sensitive Confidential Data
Level IV	Identifiable Greater than Minimal Risk Confidential Data Coded Sensitive Confidential Data
Level V	Identifiable Sensitive Confidential Data

DEFINITIONS

Anonymous Data: Data collected and recorded such that no identifier whatsoever exists to link a subject's identity to that subject's response

Coded Data: Data where identifying information has been replaced with a code and a key to decipher the code is available, which can link the identifying information to the data

Confidential Data: Data that a subject has disclosed to the investigator with the expectation that it will not be divulged to others without the subject's permission

De-identified Data: Data from which all personally identifiable information has been severed

Greater than Minimal Risk Data: Data the disclosure of which could cause greater than minimal harm or distress (such as that not encountered in daily life or during the performance of routine physicals or psychological examinations or tests).

Minimal Risk Data: Data the disclosure of which would cause minimal harm or distress (such as that encountered in daily life or during the performance of routine physicals or psychological examinations or tests).

Research Data: Human subjects' data, documentation of subject eligibility, original signed and dated consent forms (or record of consent if verbal), master keys, and findings review logs, as well as ancillary materials such as administrative and financial records.

Sensitive Data: Data the disclosure of which could have adverse consequences or put a subject at risk of criminal or civil liability or be damaging to his/her financial standing, employability, reputation, etc.

GENERAL CONSIDERATIONS FOR ALL RISK LEVELS

1. The most restrictive management option feasible should be employed.

2. Only the minimum subject identifiers – direct and indirect – necessary for the research should be collected.

3. When working with sensitive data, subject identifiers should be removed or destroyed as soon as is feasible for the research.

   Note that research data are not considered de-identified unless ALL links between the subject's identity and their data are destroyed.

4. Physical and/or electronic access to any area and/or device where research data are being stored must be limited.

5. Access to all confidential identifiable sensitive research data should be limited to investigators and key research personnel.

   Note that for student researchers, this must include the PI.

6. Strong passwords must always be used.

   See Brandeis University ITS's webpage Protect Your Data and Identity for information regarding creating strong passwords.

7. Only secure/encrypted modes of electronic transmission of research data should be used.

   Note that email and text transmissions are generally not secure and should not be used to transmit research data.

8. Computers must be protected against malware with anti-malware software approved by the Brandeis University ITS, and all software updates and patches applied.

9. The PI must report any breaches in confidentiality to the IRB within seven days of the researchers becoming aware of the event.

10. Brandeis University policy holds that human-subjects research data must be retained for a minimum of three years.

    Note that a number of policies, guidelines, rules, and regulations require longer retention of research data. See HRPP Policy #101: Data Retention for additional information.

11. When destroying research data stored on a computer, deleting the files is not enough as the deleted files can still be recovered. The deleted files must also be scrubbed from the computer so that the data are permanently erased. This may be done using commercial software approved by the Brandeis University ITS. Alternatively, the device may be degaussed or destroyed.

12. If keeping sensitive research data indefinitely, data should be de-identified, at the latest, when the current project is complete.

13. If retaining de-identified research data indefinitely, storage in a data repository should be considered.

14. If conducting an online survey, the Brandeis University preference and default is that investigators use Qualtrics.

    Note that Qualtrics gives the option for anonymization of research data, and can be set so that IP addresses (considered identifiers) are not collected.

    Note that students will no longer have access to their Qualtrics accounts once they leave Brandeis University; therefore, student researchers should use their PI's Qualtrics account and utilize the collaboration feature to develop their online surveys.

Note that Amazon's Mechanical Turk (MTurk) should be used as a recruitment tool only; Amazon has access to subjects' identifiers and survey responses when surveys are run internally to MTurk, making confidentiality an impossibility. Instead, a link to a Qualtrics survey can be embedded in the MTurk description of the study.

15. If traveling abroad, international laws and export controls regulations must be considered as they may limit the movement of research data out of the country, both physically and electronically. The principal investigator must know the applicable laws and regulations of the country in which the research will be conducted before embarking on any research and, if needed, arrangements and agreements must be in place to ensure compliance.

    Note that if conducting research in a European Union or other European Economic Area state, the data may be subject to the General Data Protection Regulations (GDPR), which may increase the level of data protection required. Contact the HRPP office for more information.

15. As research progresses, so might the risk level – appropriate data management must be used for the level of risk at each stage of the research.

DATA MANAGEMENT OPTIONS: RISK LEVEL I

When Working with Paper Documents
Paper documents such as surveys, audio transcriptions, or field notes must be stored in a secure place such as a locked file cabinet.

Note: Any signed consent forms must be stored in a separate locked cabinet from the remaining research data.

When Working with Digital Recordings
Digital recording devices/audiotapes/videotapes with recordings of interviews, field notes, etc. must be stored in a secure place such as a locked file cabinet.

Note: You can audio record directly into your Box.com account, eliminating the need for transporting and storing audio recording devices/audiotapes.

When Using Electronic Storage
When scanned or uploaded, paper documents and audio/video files must be stored in one of the following:

- Brandeis-provided Box.com account
- Brandeis-provided and Brandeis-certified file server
- Password protected computer file

When Working with Digital System Files
Digital system files such as databases, SAS/SPSS data files, or custom application record sets must be stored in one of the following:

- Brandeis-provided Box.com account
- Brandeis-provided and Brandeis-certified file server
- Password protected computer file

DATA MANAGEMENT OPTIONS: RISK LEVEL II

When Working with Paper Documents
Paper documents such as surveys, audio transcriptions, or field notes must be stored in a secure place such as a locked file cabinet in a locked office.

Note: Any signed consent forms and master keys must be stored in a separate locked cabinet from the remaining research data.

When Working with Digital Recordings
Digital recording devices/audiotapes/videotapes with recordings of interviews, field notes, etc. must be stored in a secure place such as a locked file cabinet in a locked office.

Note: You can audio record directly into your Box.com account, eliminating the need for transporting and storing audio recording devices/audiotapes.

When Using Electronic Storage

When scanned or uploaded, paper documents and audio/video files must be stored in one of the following:

- Brandeis-provided Box.com account
- Brandeis-provided and Brandeis-certified file server
- Password protected computer file

Note: When consent forms and master keys are stored digitally, they must be stored in separate accounts from the research data.

When Working with Digital System Files

Digital system files such as databases, SAS/SPSS data files, or custom application record sets must be stored in one of the following:

- Brandeis-provided Box.com account
- Brandeis-provided and Brandeis-certified file server
- Password protected computer file

Review of Findings

The safety of all research data should be reviewed and the findings logged on a regular basis.

DATA MANAGEMENT OPTIONS: RISK LEVEL III

When Working with Paper Documents

Paper documents such as surveys, audio transcriptions, or field notes must be stored in a secure place such as a locked file cabinet in a locked office.

Note: Any signed consent forms and master keys must be stored in a separate locked cabinet from the remaining research data.

Any master keys should be shredded as early as is feasible.

When Working with Digital Recordings

Digital recording devices/audiotapes/videotapes with recordings of interviews, field notes, etc. must be stored in a secure place such as a locked file cabinet in a locked office.

Note: You can audio record directly into your Box.com account, eliminating the need for transporting and storing audio recording devices/audiotapes.

When Using Electronic Storage

When scanned or uploaded, paper documents and audio/video files must be stored in one of the following:

- Brandeis-provided Box.com account
- Brandeis-provided and Brandeis-certified file server
- Password protected and encrypted computer file

Note: When consent forms and master keys are stored digitally, they must be stored in separate accounts from the research data.

When Working with Digital System Files

Digital system files such as databases, SAS/SPSS data files, or custom application record sets must be stored in one of the following:

- Brandeis-provided Box.com account
- Brandeis-provided and Brandeis-certified file server
- Password protected and encrypted computer file

Review of Findings

The safety of all research data should be reviewed and the findings logged, at a minimum, on a weekly basis.

DATA MANAGEMENT OPTIONS: RISK LEVEL IV

When Working with Paper Documents

Paper documents such as surveys, audio transcriptions, or field notes must be stored in a secure place such as a locked box in a locked file cabinet in a locked office, or a locked file cabinet in a locked office with electronic door access control and/or in sight of a security camera.

When being transported, paper documents must be secured, for example in a locked briefcase or lockbox.

Note: Any signed consent forms and master keys must be stored in a separate locked cabinet from the remaining research data – preferably in a separate room or building.

Paper documents should be scanned and shredded as early as is feasible.

When Working with Digital Recordings

Digital recording devices/audiotapes/videotapes with recordings of interviews, field notes, etc. must be stored in a secure place such as a locked box in a locked file cabinet in a locked office, or a locked file cabinet in a locked office with electronic door access control and/or in sight of a security camera.

When being transported, digital recording devices/audiotapes/videotapes must be secured, for example in a locked briefcase or lockbox.

Note: You can audio record directly into your Box.com account, eliminating the need for transporting and storing audio recording devices/audiotapes.

Audio/video files should be uploaded and originals destroyed as early as is feasible.

When Using Electronic Storage

When scanned or uploaded, paper documents and audio/video files must be stored in one of the following:

- Brandeis-provided Box.com account
- Brandeis-provided and Brandeis-certified file server

If access to the internet is not possible, use of a password protected and encrypted USB drive or anti-virus protected, password protected, and encrypted computer file may be allowable. The device (e.g., computer or USB drive) should be stored in a locked box in a locked file cabinet in a locked office, or a locked file cabinet in a locked office with electronic door access control and/or in sight of a security camera.

Note: When consent forms and master keys are stored digitally, they must be stored in separate accounts from the research data.

When Working with Digital System Files

Digital system files such as databases, SAS/SPSS data files, or custom application record sets must be stored in one of the following:

- Brandeis-provided Box.com account
- Brandeis-provided and Brandeis-certified file server
- Password protected and encrypted computer file

Review of Findings

The safety of all research data should be reviewed and the findings logged on a daily basis.

DATA MANAGEMENT OPTIONS: RISK LEVEL V

Note that paper documents, audiotapes, and videotapes should be avoided – and research data collected electronically – whenever possible.

When Working with Paper Documents

Paper documents such as surveys, audio transcriptions, or field notes must be stored in a secure place such as a locked box in a locked file cabinet in a locked office, or a locked file cabinet in a locked office with electronic door access control and/or in sight of a security camera.

When being transported, paper documents must be secured, for example in a locked briefcase or lockbox.

Paper documents should be scanned and shredded as early as is feasible.

When Working with Digital Recordings

Digital recording devices/audiotapes/videotapes with recordings of interviews, field notes, etc. must be stored in a secure place such as a locked box in a locked file cabinet in a locked office, or a locked file cabinet in a locked office with electronic door access control and/or in sight of a security camera.

When being transported, digital recordings must be secured, for example in a locked briefcase or lockbox.

Note: You can audio record directly into your Box.com account, eliminating the need for transporting and storing audio recording devices/audiotapes.

Audio/video files should be uploaded and destroyed as early as is feasible.

When Using Electronic Storage

When scanned or uploaded, paper documents and audio/video files must be stored in one of the following:

- Brandeis-provided Box.com account
- Brandeis-provided and Brandeis-certified file server

If access to the internet is not possible, use of a password protected and encrypted USB drive or anti-virus protected, password protected, and encrypted computer file may be allowable. The device (e.g., computer or USB drive) should be stored in a locked box in a locked file cabinet in a locked office, or a locked file cabinet in a locked office with electronic door access control and/or in sight of a security camera.

When Working with Digital System Files

Digital system files such as databases, SAS/SPSS data files, or custom application record sets must be stored in one of the following:

- Brandeis-provided Box.com account
- Brandeis-provided and Brandeis-certified file server
- Password protected and encrypted computer file

Review of Findings

The safety of all research data should be reviewed and the findings logged on a daily basis.